密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2016,3(4):374–381

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

CCTR 认证模式的不可证明安全性*

李玉玲[1,2,3], 王 鹏[1,2]

1. 中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093
2. 中国科学院数据与通信保护研究教育中心, 北京 100093
3. 中国科学院大学, 北京 100049
通讯作者: 王鹏, E-mail: wp@is.ac.cn

摘 要: 消息认证码是现代密码学中用以检验数据完整性和数据起源认证的重要手段. 分组密码认证模式是利用分组密码为基础部件来实现认证功能的一种工作模式. 安全和效率是消息认证码的设计过程中需要权衡的两个方面. 为了提高分组密码认证模式的效率, 2009 年, 黄玉划等人提出了一种基于链接与计数的快速认证模式(CCTR), 并从统计评估的角度验证了 CCTR 模式的安全性. 本文利用底层分组密码的特性, 分别从实际攻击的角度和可证明安全性的角度对 CCTR 模式的安全性进行了分析. 利用 CCTR 模式中部分分组密码密钥输入部分可控的特点, 我们进行选择消息攻击. 两种攻击方法只需对标签生成算法询问一次, 就可以伪造成功. 研究结果表明: 在 CCTR 模式实际使用中, 当所用分组密码具有一个和 DES 相同的性质时, CCTR 模式是不安全的; 当所用分组密码是一个有弱密钥的伪随机置换时, CCTR 模式也是不安全的. 同时表明, 原文中 CCTR 模式的安全性证明是错误的, 仅仅在伪随机置换的假设下, 不足以证明 CCTR 模式安全性.

关键词: 消息认证码; 认证模式; 分组密码; 伪随机置换
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000136

中文引用格式: 李玉玲, 王鹏. CCTR 认证模式的不可证明安全性[J]. 密码学报, 2016, 3(4): 374–381.
英文引用格式: LI Y L, WANG P. Unprovable security of CCTR authentication mode[J]. Journal of Cryptologic Research, 2016, 3(4): 374–381.

Unprovable Security of CCTR Authentication Mode

LI Yu-Ling[1,2,3], WANG Peng[1,2]

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
3. University of Chinese Academy of Sciences, Beijing 100049, China
Corresponding author: WANG Peng, E-mail: wp@is.ac.cn

Abstract: Message Authentication Code (MAC) is an important means to verify data integrity and data origin in modern cryptography. Block cipher authentication mode is a MAC based on block cipher. We do trade-off between security and efficiency in designing MAC. In order to improve the efficiency, Huang et al. proposed a MAC using chaining and counter (CCTR) mode and tested its security through statistical evaluation. In this paper, we analyze the security of CCTR by a practical attack and give a counter example against its provable

* 基金项目: 国家自然科学基金项目(61272477, 61472415)
收稿日期: 2015-12-15 定稿日期: 2016-01-24

security. We adopt the chosen-message attack by controlling the input of key to some underlying block ciphers. The two successful forgery attacks only need to query the tag-generating algorithm once. We show that CCTR is not secure when using a DES-like block cipher or a block cipher with some weak keys. We also show that the result of provable security about CCTR is wrong since it is insufficient to prove its security under the assumption of pseudorandom permutation (PRP).

Key words: Message Authentication Code; authentication mode; block cipher; Pseudorandom Permutation

1 引言

消息认证码(Message authentication codes, MAC)是一种保护数据完整性的对称密码算法. 使用MAC算法可以确保消息来自真实的发送方, 并且在传输的过程中未受到非法的篡改. 消息认证码[1]通过以下认证机制来保护消息的完整性: 首先参与通信的双方之间共享一个密钥, 通信时(这里使用 A 和 B 代表参与通信的两方), A 传送一个消息 M 给 B, 并将这一消息用 MAC 算法和共享密钥计算出一个标签, 记为 T_1, 然后将 (M,T_1) 传送给 B. 认证过程是: B 在接收后使用同样的机制计算消息 M 的标签, 记为 T_2. 如果 $T_2=T_1$, B 就认为消息 M 在由 A 传送到 B 的过程中没有被篡改; 如果不相同, B 就认为消息在传送过程中被篡改了. 同时, 由于只有拥有密钥的通信方才能计算出有效的标签, 这样就保证了消息来源的真实性.

目前的MAC算法大致可以分成三类: 第一类是基于分组密码构造的, 例如CBC-MAC[2]、OMAC[3]; 第二类是基于哈希函数构造的, 例如 HMAC[4]、NMAC[4]; 第三类是基于泛哈希函数(Universal hash function)构造的, 例如 UMAC[5]、Poly1305-AES[6]. 利用分组密码构造的 MAC 也称为分组密码认证模式, 例如本文的研究对象 CCTR 认证模式[7].

安全性是任何密码算法的核心问题. 目前有两种方法论证密码算法的安全性: 一种是讨论算法抵抗具体攻击的能力, 即如果对已知的所有攻击都是安全的, 那么可以认为这个密码算法是安全的. 常见的对称密码算法攻击包括差分攻击[8]、相关密钥攻击[9–11]、密钥恢复攻击[12–15]等等. 另一种方法是进行安全性证明. 这类证明是在基本模块安全的假设前提下, 进行上层密码方案的安全性论证. 证明的方式类似于反证法: 先假设存在有效的算法攻击上层方案, 然后在此基础上, 构造攻击基本模块的有效算法, 即将对方案的攻击归约为对基本模块的攻击, 从而只要基本模块是安全的, 方案就是安全的. 例如, 在基于分组密码的认证模式中, 通常假设所用的分组密码是一个伪随机置换(Pseudorandom Permutation, PRP), 然后在此基础上证明认证模式的安全性.

目前, 安全性证明已经成为分组密码工作模式中必不可少的一部分, 探讨底层分组密码安全假设和上层工作模式安全性之间的关系成为工作模式研究中的重要问题. 虽然在伪随机置换的假设下, 研究者给出了大量工作模式的安全性证明, 但是研究表明, 某些工作模式由于自身的设计缺陷, 不具备可证明安全性. 例如, Iwata[16]等人论证了认证模式 OMAC 的变体 OMAC1 在 PRP 假设下不具有可证明安全性. Iwata[17]等人论证了 3GPP 中的加密模式 f8 和认证模式 f9 在 PRP 假设下不具有可证明安全性, 但是在抗相关密钥攻击的伪随机置换(Related-key Pseudorandom Permutation, RK-PRP)假设下, 可以证明 f8 和 f9 的安全性[18]. 王鹏等人[19]证明了认证模式 2-key XCBC 在 PRP 假设下不具有可证明安全性, 这种模式在 RK-PRP 假设下也不具有可证明安全性.

一个安全的MAC应具有不可伪造性, 即攻击者在任意询问MAC算法之后, 仍然无法给出一条新的消息及其标签能通过认证. 例如, OMAC、CBC-MAC、HMAC 和 UMAC 等消息认证码都是在 PRP 的假设下证明其不可伪造性的.

CCTR 是黄玉划等人[7]提出的一种分组密码认证模式. 设计者的研究表明, CCTR 模式的软件实现效率比常用的认证模式(例如 CBC-MAC)快 30%左右, 从统计评估的角度验证了 CCTR 模式具有很好的伪随机性, 并且在所用分组密码是伪随机置换的假设前提下, 给出了 CCTR 模式的安全性归约证明.

但我们注意到, CCTR 模式在对分组密码的调用过程中(最后一次除外), 并没有对密钥输入部分进行任

何保护，攻击者可以完全控制这一部分的输入. 本文从底层模块的角度对CCTR模式的安全性进行了分析. 首先，如果 CCTR 底层的分组密码具有一个和 DES 相同的性质($E_{\bar{K}}(\bar{P})=\overline{E_K(P)}$, E 是分组密码，K 为密钥，P 为明文)时，那么可找到一个实际的伪造攻击. 其次，从可证明安全性的角度，如果 CCTR 底层的分组密码是一个带有弱密钥[8]的伪随机置换，那么可以利用弱密钥的特性给出一个实际攻击. 因此，本文的研究结果表明文献[7]中关于 CCTR 模式的可证明安全的结果是存在问题的，仅仅在伪随机置换的假设下，不足以证明 CCTR 模式是安全的.

本文的安排如下：第 2 节给出了所需的基本概念；第 3 节给出了 CCTR 模式的描述；第 4 节给出了 CCTR 模式的安全性分析；第 5 节是结束语.

2 基本概念

2.1 消息认证码的定义

消息认证码(MAC)是一对算法 $\Pi=(\mathrm{TG},\mathrm{VF})$, 其中

(1) TG 是标签生成算法. 输入密钥 K 和消息 M, 输出定长的标签 T, 记为 $T=\mathrm{TG}(K,S,M)$. TG 可能是一个随机的或者带状态的算法，计算过程用到一个随机串或者状态 S. 当 TG 是确定性算法时，S 是空字符串.

(2) VF 是验证算法. 输入密钥 K、消息 M、标签 T 和计算 T 时用到的随机串或者状态 S, 输出 1(表示接受)或者 0(表示拒绝). VF 是一个确定性的算法. 通常 VF 直接利用 TG 再次生成标签，并和收到的标签对比，来判断消息是否有效. 其中 K 是通信的双方事先随机生成的密钥. 为了保持一致性，我们要求 $\mathrm{VF}(K,S,M,\mathrm{TG}(K,S,M))=1$, 其中 S 是标签生成过程中用到的随机串或者状态.

2.2 不可伪造的定义

消息认证码 $\Pi=(\mathrm{TG},\mathrm{VF})$ 是不可伪造的，如果攻击者可以询问 $\mathrm{TG}(K,\cdot)$, 但是在多项式时间内无法伪造新的消息通过验证算法 VF, 其中密钥 K 是随机生成的并且只有通信双方知道. 假设攻击者是 A, 我们用 $\Pr[A^{\mathrm{TG}}\ \mathrm{forges}]$ 表示 A 伪造成功的概率. 更确切地说，如果 $\Pr[A^{\mathrm{TG}}\ \mathrm{forges}]$ 是可忽略的，那么称 $\Pi=(\mathrm{TG},\mathrm{VF})$ 是不可伪造的，即是安全的.

2.3 伪随机置换的定义

假设分组密码是 $E:\mathrm{Key}\times\{0,1\}^n\to\{0,1\}^n$, 其中 Key 是密钥空间，$n$ 是分组长度，对于任意的密钥 K, $E(K,\cdot)$ 是一个置换. 通常将 $E(K,M)$ 写为 $E_K(M)$..

在分组密码认证模式的安全性证明中，一般假设所用的分组密码是一个伪随机置换(PRP)，即当密钥随机选取时，得到的置换和随机置换是不可区分的. 这一假设最早用于 CBC-MAC 的安全性证明中[2]，之后成为论证分组密码工作模式安全性的标准假设. 以下我们记区分 E 和随机置换的算法为 A, $A^O=1$ 表示 A 可以询问问答机 O, 最后输出比特 1. $s\leftarrow_R S$ 表示从集合 S 中随机选取一个 s. $\mathrm{Perm}(n)$ 表示 $\{0,1\}^n$ 上的所有置换的集合.

定义 1(伪随机置换) 令 $E:\mathrm{Key}\times\{0,1\}^n\to\{0,1\}^n$ 是分组密码，A 区分 E 和随机置换的优势定义为:

$$\mathrm{Adv}_E^{\mathrm{prp}}(A)=\left|\Pr[K\leftarrow_R\mathrm{Key}:A^{E_K(\cdot)}=1]-\Pr[p\leftarrow_R\mathrm{Perm}(n):A^{p(\cdot)}=1]\right|$$

若对所有时间复杂度为 t、对问答机的询问不超过 q 次、询问的总比特数不超过 μ 比特的算法 A,

$$\mathrm{Adv}_E^{\mathrm{prp}}(t,q,\mu)=\max_A\left\{\mathrm{Adv}_E^{\mathrm{prp}}(A)\right\}$$

是可忽略的, 我们称分组密码 E 为伪随机置换.

3 CCTR 模式的描述

设计者将 CCTR 模式分成两种形式[7], 一种是 3 重分组的 CCTR 模式, 记为 CCTR3; 另一种是 2.5 重分组的 CCTR 模式, 记为 CCTRe. 两种形式仅仅在分组大小上有所不同, 并无本质区别. 以下给出 CCTR3 模式的描述, 如无特殊说明, 以下提到 CCTR 模式时均指 CCTR3 模式.

CCTR3 模式可以表示为: $T=\mathrm{CCTR3}(\mathrm{IV},K,M)$, 其中 IV 是初始向量, 由计数器或伪随机发生器生成, 要求不能重复, K 是密钥, M 是消息. CCTR3 用到的分组密码是 $E:\{0,1\}^{256}\times\{0,1\}^{128}\to\{0,1\}^{128}$, 即密钥长度是 256 比特, 分组长度是 128 比特的分组密码, 例如 AES-256. CCTR3 模式的标签生成算法如下:

(1) 填充: 如果消息 M 的长度是 48 字节(384 比特)的整数倍, 则不需要填充; 否则, 进行"周期补位", 即将 M 开头的若干位依次补到 M 的末尾: for $i=1$ to $48-t$, $M[L+i]=M[i]$. 其中 $M[i]$ 表示 M 的第 i 个字节, L 是 M 的字节数, $t=L \bmod 48$.

(2) 分组: 先将 M 按照 48 字节分成 n 大组, 然后将每一大组按照 16 字节分成 3 小组, 因此最终 $M=M_1M_2M_3\cdots M_{3n}$.

(3) 产生不重复的随机数: $Y_0=E_K(y)$, 其中 $y=\mathrm{IV}\|k\|L$, k 是一个 8 比特的数,表示密钥的字节数.

(4) 迭代: For $i=1$ to n, $Y_i=E_{(M_{3i-2}\oplus i)\|(M_{3i-1}+i)}(M_{3i}\oplus Y_{i-1})$.

(5) 输出: $T=\mathrm{MSB}_m[E_K(Y_n)]$, 其中 $\mathrm{MSB}_m[Y]$ 表示截取 Y 的前 m 比特.

下面给出其标签生成过程的简易示意图, 以处理两个大分组消息为例.

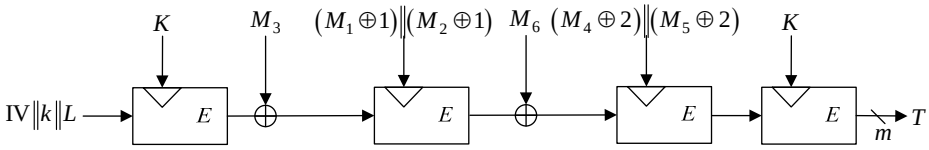

图 1 CCTR 模式的标签生成算法(处理两个大分组消息的情况)
Figure 1 The tag generation algorithm of CCTR Mode

4 CCTR 模式的安全性分析

CCTR 模式将密钥 K 分别应用到首尾两次分组密码的调用中, 这也正是整个方案的随机性来源. 第一次调用 E_K 用于 Y_0 的生成, $Y_0=E_K(\mathrm{IV}\|k\|L)$, 由于初始向量 IV 每次都不重复, 因此 $Y_0=E_K(\mathrm{IV}\|k\|L)$ 可以看成是随机的; 第二次调用: $E_K(Y_n)$, 只要 Y_n 没有和之前分组密码的输入重复, $E_K(Y_n)$ 也可以看作是随机的. 但是我们注意到, 中间的迭代过程 $Y_i=E_{(M_{3i-2}\oplus i)\|(M_{3i-1}+i)}(M_{3i}\oplus Y_{i-1})$ 调用了 n 次分组密码, 每次调用中分组密码 E 的密钥输入部分是不含密钥 K 的, 在选择明文攻击下, E 的密钥输入部分是完全可控的, 明文输入部分是部分可控的. CCTR 模式的这一特点为下面的攻击提供了便利.

对于对称算法而言, 其在弱密钥集上表现的特性会有所不同, 敌手可利用弱密钥的特性进行伪造攻击、区分攻击和密钥恢复攻击等等. 例如, 文献[9]中利用弱密钥的特性对 XCB、HCTR 和 HCH 等方案进行区分攻击, 文献[20,21]对 GCM 方案进行伪造攻击和密钥恢复攻击. 在 4.2 部分, 本文利用伪随机置换的

弱密钥对 CCTR 模式进行了伪造攻击.

在对 CCTR 模式的分析中, 本文选取的消息都是 6 小组(两大分组、96 字节)长度的, 这样就不必考虑 CCTR 模式的填充方式, 并且 Y_0 的生成也不受消息长度的影响.

我们给出了两种攻击方法, 分别针对 CCTR 模式中分组密码可能存在的特征和伪随机置换可能存在的弱点. 两种攻击方法的共同特点是, 找到两个不同的消息 M 和 M', 其对应的标签相同, 其中 M' 是通过修改 M 得到的. 这样我们可以先询问 M, 得到标签 T, 然后伪造 (M',T), 显然伪造成功的概率为 1. 例如在现实的攻击环境中, 我们截获到了消息 (M,T), 这时就可以将其替换成 (M',T) 继续发给接收方, 接收方收到消息后会验证其是有效的.

4.1 利用分组密码可能的特征进行攻击

CCTR 模式中间迭代过程的特点给攻击带来很多便利之处. 下面给出一种可能存在的攻击. CCTR 模式必须用到具体的分组密码才能实现, 假设我们用到了类似于 DES 的分组密码.

众所周知, DES 有如下性质[22]: $E_{\overline{K}}(\overline{P})=\overline{E_K(P)}$ (当密钥和明文都取补时, 相应的密文也取补), 其中 $\overline{P}$ 表示 P 的补, 即将 P 中的 0 变成 1, 1 变成 0. 假设 CCTR 模式用到的分组密码也具有这样的性质.

攻击者首先询问一条 6 小分组(96 字节)的消息 $M=M_1M_2M_3M_4M_5M_6$, 得到标签 T. 按照之前的描述, T 计算过程如下:

$$
\begin{aligned}
&Y_0=E_K(y)\\
&Y_1=E_{(M_1\oplus 1\|M_2+1)}(M_3\oplus Y_0)\\
&Y_2=E_{(M_4\oplus 2\|M_5+2)}(M_6\oplus Y_1)\\
&T=\mathrm{MSB}_m\left[E_K(Y_2)\right]
\end{aligned}
$$

注意到, 在计算 T 的过程中一共调用了四次分组密码 E, 而且在中间两次调用中, E 的密钥和明文部分的输入都在攻击者的控制中. 下面对原来的消息 M 进行修改. 将 M_1 修改为 $M_1'=\overline{M_1}$, 将 M_2 修改为 $M_2'=\overline{M_2+1}-1$, 将 M_3 修改为 $M_3'=\overline{M_3}$, 那么在第二次调用中, E 的密钥和明文部分的输入都变为原来的补. 这样, 按照 DES 的性质, E 的第二次输出是原来的补, 即 Y_1 变为 $Y_1'=\overline{Y_1}$.

我们通过第三次分组密码调用中对明文部分的输入的控制, 将 M_6 修改为 $M_6'=\overline{M_6}$, 那么 $M_6'\oplus Y_1'=\overline{M_6}\oplus\overline{Y_1}=M_6\oplus Y_1$, 即 E 的第三次明文部分的输入和原来的一样. 同时我们让其它部分的消息保持不变: $M_4'=M_4$, $M_5'=M_5$. 那么第四次调用分组密码调用(即 E_K)的输入和原来的一样, 修改后消息 $M'=M_1'M_2'M_3'M_4'M_5'M_6'$ 对应的标签仍然是 T .

这样, 攻击者可以成功(概率为 1)伪造出消息组 (M',T).

4.2 利用伪随机置换可能的弱密钥进行攻击

分组密码是伪随机置换(PRP)的假设保证了当密钥随机选择时, 得到的置换和一个完全随机的置换是不可区分的, 而当分组密码出现一个弱密钥时, 并不会对分组密码的伪随机性造成影响. 然而, 当存在弱密钥的算法作为方案的底层部件时, 则有可能使得方案不安全. 例如, 文献[20,21]利用底层多项式函数的弱密钥, 发起了对 GCM 的伪造攻击. 在 CCTR 模式中, 我们可以通过构造一个带有弱密钥的伪随机置换, 说明基于此的 CCTR 是不安全的.

假设分组密码 E 是一个伪随机置换(PRP), 我们构造一个新的带弱密钥的分组密码 E',

$$E'_K(P)=\begin{cases}P, & K=0^{256}\\ E_K(P), & K\neq 0^{256}\end{cases}$$

我们构造的分组密码增加了一个弱密钥 0^{256}, 在此密钥下, 分组密码变成了一个恒等变换; 对于其它密钥, 与原来的分组密码保持一致. 伪随机置换定义的是密钥随机选取时得到的置换和随机置换的不可区分性, 我们仅仅改变了 E 在一个密钥下的置换, 在密钥随机的情况下, 碰上这一密钥的概率很小 $\left(1/2^{256}\right)$, 因此得到的 E' 继承了 E 的伪随机性质. 下面证明, 当 E 是 PRP 时, E' 也是 PRP.

证明: 对于任意时间复杂度为 t 、对问答机的询问不超过 q 次、询问的总比特数不超过 μ 比特的算法 A 而言, A 区分 E 和随机置换的优势为:

$$\begin{aligned}\mathrm{Adv}_E^{\mathrm{prp}}(A)&=\left|\Pr\left[K\leftarrow_R \mathrm{Key}: A^{E_K(\cdot)}=1\right]-\Pr\left[p\leftarrow_R \mathrm{Perm}(n): A^{p(\cdot)}=1\right]\right|\\&=\left|\Pr_K\left[A^{E_K(\cdot)}=1\middle|K=0^{256}\right]\Pr_K\left[K=0^{256}\right]+\Pr_K\left[A^{E_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|\\&=\left|\Pr_K\left[A^{E_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]+\frac{\Pr_K\left[A^{E_K(\cdot)}=1\middle|K=0^{256}\right]}{2^{256}}\right|\end{aligned}$$

A 区分 E' 和随机置换的优势为:

$$\begin{aligned}\mathrm{Adv}_{E'}^{\mathrm{prp}}(A)&=\left|\Pr\left[K\leftarrow_R \mathrm{Key}: A^{E'_K(\cdot)}=1\right]-\Pr\left[p\leftarrow_R \mathrm{Perm}(n): A^{p(\cdot)}=1\right]\right|\\&=\left|\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K=0^{256}\right]\Pr_K\left[K=0^{256}\right]+\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|\\&\leqslant\left|\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K=0^{256}\right]\Pr_K\left[K=0^{256}\right]\right|+\left|\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|\\&\leqslant\left|\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|+\frac{\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K=0^{256}\right]}{2^{256}}\\&=\left|\Pr_K\left[A^{E_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|+\frac{\Pr_K\left[A^{E'_K(\cdot)}=1\middle|K=0^{256}\right]}{2^{256}}\end{aligned}$$

所以我们得到:

$$\begin{aligned}\mathrm{Adv}_{E'}^{\mathrm{prp}}(A)&\leqslant\left|\Pr_K\left[A^{E_K(\cdot)}=1\middle|K\neq 0^{256}\right]\Pr_K\left[K\neq 0^{256}\right]-\Pr\left[A^{p(\cdot)}=1\right]\right|+\frac{1}{2^{256}}\\&\leqslant\mathrm{Adv}_E^{\mathrm{prp}}(A)+\frac{\Pr_K\left[A^{E_K(\cdot)}=1\middle|K=0^{256}\right]}{2^{256}}+\frac{1}{2^{256}}\\&\leqslant\mathrm{Adv}_E^{\mathrm{prp}}(A)+\frac{1}{2^{255}}\end{aligned}$$

根据 E 是伪随机置换, 我们有:

$$\mathrm{Adv}_{E'}^{\mathrm{prp}}(t,q,\mu)=\max_A\left\{\mathrm{Adv}_{E'}^{\mathrm{prp}}(A)\right\}\leqslant\max_A\left\{\mathrm{Adv}_E^{\mathrm{prp}}(A)+\frac{1}{2^{255}}\right\}=\mathrm{Adv}_E^{\mathrm{prp}}(t,q,\mu)+\frac{1}{2^{255}}\leqslant\frac{1}{2^{255}}+\varepsilon$$

因此, E' 也是伪随机置换.

以下在不引起歧义的情况下, 同时将字符串看成 128 比特的整数. 例如整数 1 表示 $0^{127}\|1$, 整数 $2^{128}-1$ 表示 1^{128}. 本文利用 E' 的这一弱点, 对 $\mathrm{CCTR}[E']$ 进行攻击. 同上面的攻击一样, 我们先询问一个有 6 小分组(96 字节)的消息 $M=M_1M_2M_3M_4M_5M_6$, 其中 $M_1=1, M_2=2^{128}-1, M_4=2, M_5=2^{128}-2$, 得到标签 T. 攻击者可以成功伪造消息 (M',T), 其中 $M'=M'_1M'_2M'_3M'_4M'_5M'_6$, $M'_i=M_i\ (i=1,2,4,5)$, $M'_3=M_3\oplus 1$, $M'_6=M_6\oplus 1$.

下面验证 $T'=T$. 根据条件, 在生成标签 T 的过程中, 中间两次调用分组密码 E', 其输入的密钥全为 0,

于是 E' 变为恒等置换，于是有:

$$\begin{aligned}
&Y_0 = E'_K\left(y\right)\\
&Y_1 = E'_{0^{256}}\left(M_3 \oplus Y_0\right) = M_3 \oplus Y_0\\
&Y_2 = E'_{0^{256}}\left(M_6 \oplus Y_1\right) = M_3 \oplus M_6 \oplus Y_0\\
&T = \mathrm{MSB}_m\left[E'_K\left(Y_2\right)\right] = \mathrm{MSB}_m\left[E'_K\left(M_3 \oplus M_6 \oplus Y_0\right)\right]
\end{aligned}$$

对于消息 $M' = M'_1M'_2M'_3M'_4M'_5M'_6$，依旧使得中间两次调用分组密码 E' 的输入密钥全为 0，且满足 $M'_3 \oplus M'_6 = M_3 \oplus M_6$，于是有:

$$\begin{aligned}
&Y'_0 = E'_K\left(y\right) = Y_0\\
&Y'_1 = E'_{0^{256}}\left(M'_3 \oplus Y'_0\right) = M'_3 \oplus Y_0\\
&Y'_2 = E'_{0^{256}}\left(M'_6 \oplus Y'_1\right) = M'_3 \oplus M'_6 \oplus Y_0 = M_3 \oplus M_6 \oplus Y_0\\
&T' = \mathrm{MSB}_m\left[E'_K\left(Y'_2\right)\right] = \mathrm{MSB}_m\left[E'_K\left(M_3 \oplus M_6 \oplus Y_0\right)\right] = T
\end{aligned}$$

这样，我们构造了一个特殊的带弱密钥的伪随机置换，而在此基础上的 CCTR 模式是不安全的. 因此，以上攻击说明了，仅仅在伪随机置换的假设下，不足以证明 CCTR 模式是安全的. 进一步，当 E 是抗相关密钥攻击的伪随机置换(RK-PRP)时，也很容易证明 E' 也是 RK-PRP. 这说明即使假设分组密码是更强的 RK-PRP，也无法证明 CCTR 模式是安全的.

5 结束语

本文从底层分组密码的角度对 CCTR 模式的安全性进行了分析. 研究结果表明，可以利用分组密码的某些特征对 CCTR 模式进行具体有效的攻击，同时通过构造一个特殊的伪随机置换，说明了文献[7]给出的安全性证明的条件是不充分的，仅仅在伪随机置换的假设下，不可能证明 CCTR 模式是安全的.

从目前的两种攻击方式看，CCTR 的安全漏洞在于其密钥的应用方式，特别是中间迭代过程中密钥的缺失. 如果在 CCTR 的中间迭代过程加入密钥，即 $Y_i = E_{K\oplus\left(\left(M_{3i-2}\oplus i\right)\|\left(M_{3i-1}+i\right)\right)}\left(Y_{i\text{-}1} \oplus M_{3i}\right)$，本文给出的两种攻击方式将失效. 并且我们可以参考文献[23]的思路，证明在 RK-PRP 假设下，这种修改是安全的.

文献[7]用大量篇幅讨论了 CCTR 模式的统计特征，例如输出服从均匀分布，二进制矩阵秩、频谱、非重叠字匹配、重叠字匹配、Maurer 通用统计等测试结果都满足要求，从而从统计评估的角度验证了 CCTR 模式具有很好的伪随机性. 但是应该看到，CCTR 模式的统计特征并不能保证其安全性. 密码方案的安全性还是应该从具体攻击或者可证明安全性的角度去论证.

需要说明的是，本文并没有说明利用其它分组密码的 CCTR 模式是不安全的，例如,利用 AES-256 构造的 CCTR 模式，并不存在 $E_{\overline{K}}\left(\overline{P}\right) = \overline{E_K\left(P\right)}$ 的特质，因此并不能说明它是不安全的. 但是潜在的攻击和可证明安全性的缺失，说明 CCTR 模式存在一定的安全隐患.

References

[1] WANG D Y, LING D D, WU W L. Research on message authentication codes[J]. Journal of Communication and Computer, 2005, 2(10): 76–81.
王大印, 林东岱, 吴文玲. 消息认证码的研究[J]. 通讯和计算机, 2005, 2(10): 76–81.

[2] BELLARE M, KILIAN J, ROGAWAY P. The security of cipher block chaining[C]. In: Advances in Cryptology—CRYPTO 1994. Springer Berlin Heidelberg, 1994: 341–358.

[3] IWATA T, KUROSAWA K. OMAC: One-key CBC MAC[C]. In: Fast Software Encryption—FSE 2003. Springer Berlin Heidelberg, 2003: 129–153.

[4] BELLARE M. New proofs for NMAC and HMAC: Security without collision-resistance[C]. In: Advances in Cryptology—CRYPTO 2006, Springer Berlin Heidelberg, 2006: 602–619.

[5] BLACK J, HALEVI S, KRAWCZYK H, et al. UMAC: Fast and secure message authentication[C]. In: Advances in Cryptology—CRYPTO 1999. Springer Berlin Heidelberg, 1999: 216–233.
[6] BERNSTEIN D J. The Poly1305-AES message-authentication code[C]. In: Fast Software Encryption—FSE 2005. Springer Berlin Heidelberg, 2005: 32–49.
[7] HUANG Y H, HU A Q, WANG J D. Chaining & counter-based block cipher mode for authentication[J]. Journal on Communications, 2009, 30(7): 99–105.
黄玉划, 胡爱群, 王建东. 基于链接与计数的分组密码认证模式[J]. 通信学报, 2009, 30(7): 99–105.
[8] HU H J, JIN C H, LI X R. Improved impossible differential attack on 7-round AES-128[J]. Journal of Cryptologic Research, 2015, 2(1): 92–100.
胡弘坚, 金晨辉, 李信然. 改进的 7 轮 AES-128 的不可能差分攻击[J]. 密码学报, 2015, 2(1): 92–100.
[9] SUN Z L, WANG P, ZHANG L T. Weak-key and related-key analysis of hash-counter-hash tweakable enciphering schemes[C]. In: the 20th Australasian Conference on Information Security and Privacy—ACISP 2015. Springer International Publishing, 2015: 3–19.
[10] LIU A S, WANG M Q, LI Y B. Related-key differential cryptanalysis of KATAN famil[J]. Journal of Cryptologic Research, 2015, 2(1): 77–91.
刘爱森, 王美琴, 李艳斌. KATAN 密码算法的相关密钥差分攻击[J]. 密码学报, 2015, 2(1): 77–91.
[11] PEYRIN T, SASAKI Y, WANG L. Generic related-key attacks for HMAC[C]. In: Advances in Cryptology—CRYPTO 2012. Springer Berlin Heidelberg, 2012: 580–597.
[12] MAVROMATI C. Key-recovery attacks against the MAC algorithm Chaskey[C]. In: the 22nd Conference on Selected Areas in Cryptography—SAC 2015. Springer Berlin Heidelberg, 2015.
[13] GUO J, PEYRIN T, SASAKI Y, et al. Updates on generic attacks against HMAC and NMAC[C]. In: Advances in Cryptology —CRYPTO 2014. Springer Berlin Heidelberg, 2014: 131–148.
[14] GUO J, SASAKI Y, WANG L, et al. Equivalent key recovery attacks against HMAC and NMAC with Whirlpool Reduced to 7 rounds[C]. In: Fast Software Encryption—FSE 2014. Springer Berlin Heidelberg, 2014: 571–590.
[15] HANDSCHUH H, PRENEEL B. Key-recovery attacks on universal hash function based MAC algorithms[C]. In: Advances in Cryptology—CRYPTO 2008. Springer Berlin Heidelberg, 2008: 144–161.
[16] IWATA T, KUROSAWA K. On the security of a new variant of OMAC[C]. In: Information Security and Cryptology—ICISC 2003. Springer Berlin Heidelberg, 2003:67–78.
[17] IWATA T, KUROSAWA K. On the correctness of security proofs for the 3GPP confidentiality and integrity algorithms[C]. In: Cryptography and Coding 2003. Springer Berlin Heidelberg, 2003: 306–318.
[18] IWATA T, KOHNO T. New security proofs for the 3GPP confidentiality and integrity algorithms[C]. In: Fast Software Encryption—FSE 2004. Springer Berlin Heidelberg, 2004: 427–445.
[19] WANG P, FENG D G, WU W L, et al. On the Unprovable security of 2-Key XCBC[C]. In: Information Security and Privacy—ACISP 2008. Springer Berlin Heidelberg, 2008: 230–238.
[20] PROCTER G, CID C. On weak keys and forgery attacks against polynomial-based MAC schemes[C]. In: Fast Software Encryption—FSE 2013. Springer Berlin Heidelberg, 2013: 287–304.
[21] ZHU B, TAN Y, GONG G. Revisiting MAC forgeries, weak keys and provable security of Galois/Counter mode of operation[C]. In: The 12th International Conference on Cryptology and Network Security—CANS 2013. Springer International Publishing, 2013: 20–38.
[22] HELLMAN M E, MERKLE R, SCHROEPPEL R, et al. Results of an initial attempt to cryptanalyze the NBS data encryption standard[R]. Technical report, Stanford University, U.S.A., September 1976.
[23] YASUDA K. Boosting Merkle-Damgård hashing for message authentication[C]. In: Advances in Cryptology—ASIACRYPT 2007. Springer Berlin Heidelberg, 2007: 216–231.

作者信息

李玉玲(1990–), 广东深圳人, 硕士. 主要研究领域为消息认证码的设计与分析.
E-mail: liyuling@iie.ac.cn

王鹏(1976–), 博士, 副研究员. 主要研究领域为对称密码方案的设计与分析.
E-mail: wp@is.ac.cn