计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20150546
53(11):2465-2474,2016

基于白盒密码的 DCAS 终端安全芯片方案

许 涛[1,2] 武传坤[1] 张卫明[3]
[1](信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)
[2](中国科学院大学 北京 100049)
[3](中国科学技术大学信息科学技术学院 合肥 230026)
(xutao@iie.ac.cn)

A White-Box-Cryptography-Based Scheme for the Secure Chip of DCAS Terminal

Xu Tao[1,2], Wu Chuankun[1], and Zhang Weiming[3]
[1](*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)
[2](*University of Chinese Academy of Sciences*, *Beijing* 100049)
[3](*School of Information Science and Technology*, *University of Science and Technology of China*, *Hefei* 230026)

Abstract In the technical specification of downloadable conditional access system (DCAS) issued by the State Administration of Radio, Film and Television of China (SARFT) in 2012, all cryptographic operations in a terminal are built into a secure chip and protected with hardware-based security technologies. Too much protected black-box contents in the secure chip, however, will lower the universality and flexibility of the chip, and add the cost of research and development. Thus, an improved scheme for the secure chip of DCAS terminal is proposed, which is based on white-box cryptography. The main idea is to replace the key ladder inside the chip by a software-based white-box decryption module outside the chip and an external encoding inside the chip. An algorithm of generating external encoding is put forward, which is executed in the secure chip and based on the protected secret key and the external input parameters. The decryption and authentication processes in the terminal are redesigned. Compared with the original scheme in the DCAS technical specification, the improved scheme not only overcomes the aforementioned deficiencies, but also provides two extra benefits: the decryption algorithm can be renewed while the service key is being downloaded from the network; the new authentication process can verify the legitimacy as well as the uniqueness of a DCAS terminal.

Key words conditional access system (CAS); downloadable conditional access system (DCAS); secure chip; white-box cryptography; external encoding

摘 要 在国家广电总局 2012 年发布的可下载条件接收系统(downloadable conditional access system, DCAS)技术规范中,终端的密码操作都被置于安全芯片内,用安全硬件技术加以保护.然而安全芯片中过多的黑盒内容降低了芯片的通用性,增加了研发成本.因此提出一种基于白盒密码的 DCAS 安全

收稿日期:2015-06-15;修回日期:2015-09-16
基金项目:中国科学院战略性先导科技专项(XDA06010701);国家自然科学基金项目(61170234);国家"八六三"高技术研究发展计划基金项目(2013AA014002)
This work was supported by the State Priority Research Program of the Chinese Academy of Sciences (XDA06010701), the National Natural Science Foundation of China (61170234), and the National High Technology Research and Development Program of China (863 Program) (2013AA014002).
通信作者:武传坤(ckwu@iie.ac.cn)

芯片改进方案,利用芯片外的白盒解密软件模块和芯片内的外部编码,替换原方案中的层级密钥模块,并给出了一种在安全芯片内根据参数生成外部编码的算法,重新设计了 DCAS 终端的解密和握手验证过程. 改进后的方案不但弥补了技术规范中原方案的缺点,还增加了如下优点:解密算法与业务密钥都包含在白盒密码模块内,可以同时通过网络下载更新;握手验证过程不仅对 DCAS 终端设备进行可用性验证,还能够进行唯一性验证.

关键词 条件接收系统;可下载条件接收系统;安全芯片;白盒密码;外部编码

中图法分类号 TP309

条件接收系统(conditional access system, CAS)对数字电视广播业务进行控制和授权,确保仅当用户满足特定的条件时才能正常使用该业务. 在 CAS 技术的早期,客户端被固化在机顶盒硬件中. 为了抵抗某种盗版攻击或者增加新的服务,系统运营商需要更换所有用户的机顶盒. 为了解决这个问题,目前大部分运营商采用了分离式的安全模块,即机顶盒+智能卡的方式. 这种方式允许系统运营商在升级 CAS 终端应用或者更换 CAS 时不用替换整个机顶盒. 然而机顶盒+智能卡的方式并不能改变当前 CAS 终端上软硬件捆绑、难以实施标准化和智能化的局面. 随着网络技术的发展,在数字电视广播网络内封闭发展的有线电视系统面临巨大的挑战,越来越多带有屏幕的智能终端正在对传统的有线电视起替代作用. 于是,能够在智能平台上运行的可下载 CAS(downloadable CAS, DCAS)受到了人们的关注.

DCAS 使用户能够通过网络下载 CAS 客户端到本地设备,包括机顶盒、智能电视、PC、平板电脑和智能手机等任何符合 DCAS 终端标准的设备. 依托 DCAS,数字电视运营商可以摆脱单纯依赖机顶盒开展业务的模式. 2012 年 3 月,为了规范我国的 DCAS 发展,广电总局颁布了《可下载条件接收系统技术规范》(以下简称《DCAS 技术规范》)[1],规定了 DCAS 的总体要求、安全机制、系统架构和功能、终端系统和终端安全芯片等内容.

下载到智能终端中的 CAS 终端软件,其运行环境是不安全的. 潜在的攻击者可能是从网络下载的恶意软件或者终端的持有者. 所以,DCAS 终端的设计者必须以如下假设作为设计前提:攻击者可以任意观察与控制软件的运行、用逆向工程的方法分析软件模块以及任意篡改软件. 这样的运行环境被称为白盒攻击环境.

在白盒攻击环境下,若 CAS 终端软件中的解密密钥以变量的形式存放在存储器中,则很容易被攻击者直接抓取并利用. 为了抵抗这种攻击,《DCAS 技术规范》将 DCAS 终端的解密/解扰操作都放置在安全芯片内. 整个终端的安全基础建立在用硬件技术对安全芯片进行保护之上. 但是这样的做法使得安全芯片内的黑盒内容过多,限制了芯片使用时的灵活性和通用性,芯片的研发成本也高.

白盒密码[2]是为了抵抗白盒攻击而提出的一项技术,其主要手段是在密码算法的软件实现中对密钥进行隐藏,使得密钥不会直接出现在存储器中. 本文针对《DCAS 技术规范》中 DCAS 终端安全芯片的设计,提出了一种基于白盒密码的改进,将安全芯片中的层级解密功能交由芯片外的白盒密码软件模块和芯片内的外部编码配合完成,并给出了一种在芯片内派生外部编码的算法. 与原设计相比,改进后的 DCAS 芯片通用性增加、研发成本降低,并且新的握手验证过程还可以用来判断终端是否是与安全芯片对应的唯一合法终端.

1 DCAS 终端安全芯片

1.1 CAS 的安全原理

CAS 由前端、传输网络与终端组成,主要实现功能有 3 层:加扰层、节目授权控制层和用户授权管理层. 图 1(a)展示了目前被大多数运营商采用的、终端是机顶盒+智能卡的 CAS 架构[3].

加扰层以控制字(control word, *CW*)为初始化密钥,通过加扰器对节目流进行加扰. 为提高安全性,*CW* 通常以 5～30 s 为周期进行变换,不同节目采用不同的控制字. 节目授权控制层用该节目的业务密钥(service key, *SK*)对 *CW* 进行加密,生成节目授权控制消息(entitlement control message, ECM). 用户授权管理层用个人分配密钥(personal distribution key, *PDK*)对 *SK* 进行加密,生成用户授权管理消息(entitlement management message, EMM). 终端的 *PDK* 一般由运营商在分发前通过

专用设备烧录入智能卡的 EPROM 中.

传输网络中的传输流格式,如图 1(b)所示. 每个节目流都有专属的 ECM 消息. 所有用户的 EMM 消息在 EMM 流中被循环广播. 当然,除了密文形式的 SK 和 CW,EMM 和 ECM 还包含其他与节目授权控制有关的信息[4].

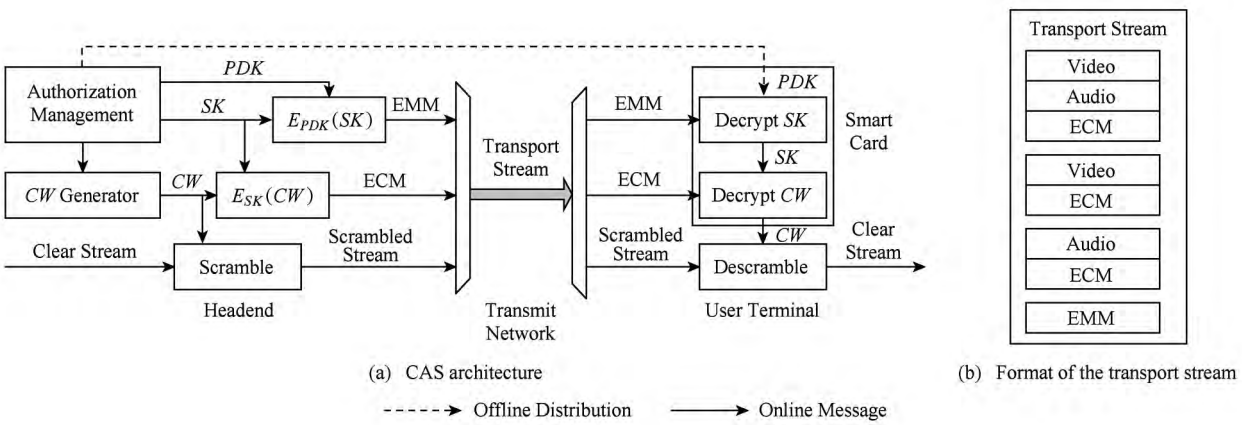

Fig. 1　CAS architecture and format of the transport stream.

图 1　CAS 架构及传输流格式

终端接收到传输流后,利用本地的 PDK 解密从 EMM 和 ECM 中获取的 $E_{PDK}(SK)$和 $E_{SK}(CW)$:$SK=D_{PDK}(E_{PDK}(SK))$,$CW=D_{SK}(E_{SK}(CW))$. 最后得到的 CW 将用于节目的解扰.

1.2　DCAS 终端安全芯片

目前,数字电视传输网络向双向转变,服务提供商在双向通信网络下提供了更多的增值业务,因而对安全保障的要求越来越高. 作为 CAS 发展方向的 DCAS 在双向通信网络中提供了动态安全体系结构以及容纳多种智能设备的可能.

《DCAS 技术规范》[1]中的 DCAS 架构与智能卡 CAS 相比,前端部分增加了认证代理服务器、DCAS 控制服务器和下载分发服务器等,同时还连接可信认证系统;终端部分取消了智能卡,并在主芯片之外增加了 1 个安全芯片. 节目流在前端和终端的加密/解密流程与前述的 CAS 原理一致. 本节重点介绍《技术规范》中的 DCAS 终端安全芯片方案.

技术规范中 DCAS 终端安全芯片的功能见图 2,其中包括一次性编程区(one time programmable area, OTP)、根密钥派生、层级密钥和解扰及解码等模块.

安全芯片的工作流程如下:1)芯片上电后,OTP 用还原函数将内置的加密安全芯片密钥(encrypted secure chipset key, $ESCK$)还原成安全芯片密钥(secure chipset key, SCK),并提供给根密钥派生模块,用于生成根密钥 $K3$;2)层级密钥模块将根密钥 $K3$ 用于对输入的已加密的密钥进行分层解密和处理握手认证流程;3)最终解密得到的 CW 被送至解扰及解码模块,用来对加扰的业务进行解扰和解码. 在安全芯片工作时,除了内置的唯一标识 $Chip\text{-}ID$ 和芯片返回的握手消息,主芯片不能通过驱动读取安全芯片内的其他信息.

根密钥派生模块根据输入的服务商系统标识($Vendor\_SysID$)及芯片内的 SCK,派生出根密钥. 任何一家服务商均通过此派生机制生成不同的根密钥,此方式规避了嵌入单一根密钥的安全风险.

芯片的层级密钥模块是 3 层结构,与 2 层结构相比,在终端用户数量很多的情况下,EMM 流中循环广播的数据量会相对较少. 层级密钥模块的密码算法可选用 TDES,AES,SMS4 等.

层级密钥模块的分层解密流程为

1) 接收密文 $E_{K3}(K2)$,使用根密钥 $K3$ 解密,得到 $K2=D_{K3}(E_{K3}(K2))$;

2) 接收密文 $E_{K2}(K1)$,使用 $K2$ 解密,得到 $K1=D_{K2}(E_{K2}(K1))$;

3) 接收密文 $E_{K1}(CW)$,使用 $K1$ 解密,得到 $CW=D_{K1}(E_{K1}(CW))$.

其中,$K1$ 相当于 1.1 节中介绍的业务密钥 SK.

层级密钥模块中的握手认证流程为

1) 接收密文 $E_{K3}(K2)$,使用根密钥 $K3$ 解密,得到 $K2=D_{K3}(E_{K3}(K2))$;

2) 使用 $K2$ 解密 $K2$,生成 $D_{K2}(K2)$,记为 A;

3) 接收握手认证消息 $Nonce$,使用 A 解密,得到 $D_A(Nonce)$;

4) 将 $D_A(Nonce)$返送回前端.

这个握手认证过程仅能够验证:终端具有解密 CW 的能力,是可以正常使用的.

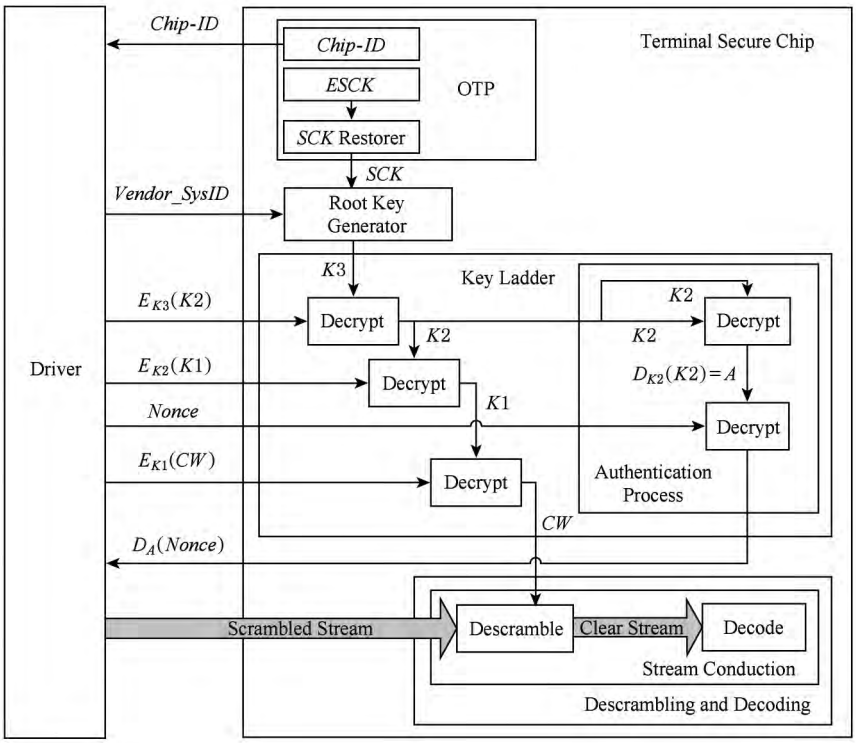

Fig. 2 The specification for the secure chip of DCAS terminal.

图 2 技术规范中的 DCAS 终端安全芯片方案

推广 DCAS 的瓶颈是终端安全芯片，因为芯片是标准的载体. 然而在《DCAS 技术规范》中，过多的黑盒内容限制了芯片在使用时的灵活性和通用性，增加了芯片成本，不利于推广. 本文尝试减少终端安全芯片中的内容，用白盒密码将层级密钥模块在安全芯片外用纯软件形式实现.

2 白盒密码

各类消费性电子产品是白盒攻击的主要对象，其中也包括符合 DCAS 规范的终端设备. 为了在白盒攻击环境中保护密码算法中的密钥，Chow 等人[2,5]提出了白盒密码的概念，并给出了 DES 和 AES 加密算法的白盒实现. 他们所用的方法仍是目前创建白盒密码应用的主要方法，即：将原密码算法用包含密钥的查找表网络实现，用随机双射对单个查找表进行编码保护，并利用外部编码把算法边界扩展到包含白盒密码模块的容器中.

本节中，我们首先介绍基于查找表网络的白盒密码及其当前的研究进展，然后介绍一种在智能终端中实际应用白盒密码的模式.

2.1 查找表网络

在软件实现时，AES 等密码算法的代换和扩散等操作可以用查找表来完成. 此时，如果密钥和某些查找表结合而不是被单独存储，攻击者便无法直接观察到密钥. 但是这样的隐藏不足以阻止攻击者轻易提取密钥信息，查找表还需要被进一步保护.

Chow 等人[2]利用编码的方法保护查找表，如图 3(a)所示. 令 X 和 Y 是 2 个查找表. ①所示的复合操作 $Y\circ X=Y(X(c))$ 表示：对输入值 c，在 X 之后执行 Y，符号 $\circ$ 表示操作的合成，编码是随机选择的双射. ②展示了如何利用输入编码 F 和输出编码 H 混淆查找表 X 和 Y 的内容. 如图 3 所示，X 和 Y 被新查找表 $X\circ F^{-1}$ 和 $H\circ Y$ 代替. ③展示如何利用编码 G 使 2 个表之间的结果也得到保护. 这样原来在存储器中的 2 个表 X 和 Y 被代替为编码后的 $X'=G\circ X\circ F^{-1}$ 和 $Y'=H\circ Y\circ G^{-1}$. 经过编码后的查找表，只要 F,G,H 保持未知，攻击者就不能轻易获得查找表 X 和 Y 中隐藏的密钥信息.

编码后的查找表组成了白盒密码模块. 整体来看，用 Chow 等人的方法实现的白盒密码是如图 3(c)所示的查找表网络. 将输入的分组依次用网络中的查找表作用，便得到加密/解密的结果.

为了防止攻击者将白盒密码模块整体窃取并利用，Chow 等人引入了外部编码，如图 3(b). 为了抵消外部编码的作用，在白盒密码模块开始或结束的

位置需要额外插入若干与密钥无关的查找表. 外部编码位于运行白盒密码模块的容器中,并用硬件或软件技术保护,使攻击者不能轻易获得. 外部编码与密钥无关,但是如果不知道外部编码,攻击者即使窃取了白盒密码模块,脱离了原来的容器后,也不能正常使用.

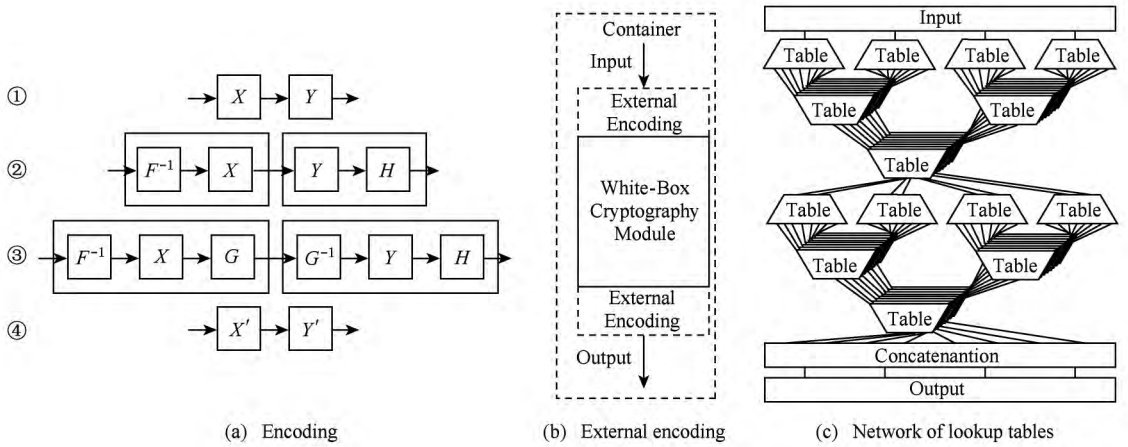

Fig. 3　Encoding, external encoding, network of lookup tables.

图 3　编码、外部编码及查找表网络

2.2　白盒密码的研究进展

Chow 等人的白盒 AES 和 DES 公布后,很快就遭到破解[6-8],Lepoint 等人[9]对白盒 AES 给出最小代价是 2^{22} 的攻击方法. 为了增加白盒 AES 的安全性,一些改进方案[10-11]被提出,但最后都被证明是不安全的[9, 12]. Michiels 等人[13]甚至给出了 1 个通用的攻击,证明将已有的 SLT 型分组密码算法用 Chow 等人的方法转成白盒密码是不安全的. 因为这些算法在设计之初并没有考虑在白盒攻击环境下运行,固定结构的代换和扩散层使得这些密码算法的白盒实现很容易被破解.

但是白盒密码技术在不断发展,新的方法不断被提出,例如:构建具有密钥相关的代换和扩散层的类 AES 白盒密码、混淆白盒密码中每轮的边界等. 新方法可以被用来抵抗已知的攻击. 白盒密码的设计者不再将思路局限于已有密码算法的白盒化,而是在尝试设计一开始就着眼于防范白盒攻击的白盒密码. 总之,白盒密码技术仍然是一项值得期待的技术.

2.3　白盒密码的应用

目前,智能终端设备的运算能力越来越接近 PC,一些原来用于 PC 的攻击技术开始转移到这些智能终端上. 由于某些移动操作系统的开放性,例如安卓,其上运行的软件应用极易遭受白盒攻击. 本节以安卓手机为例,介绍了一种实际应用白盒密码的模式:受硬件技术保护的外部编码配合软件形式的白盒密码应用模块.

如图 4 所示,外部编码在 USIM 卡中,攻击者不能直接读取. 需要加密/解密的数据先被送往 USIM 卡,经外部输入编码处理后,回传给安卓系统内包含白盒密码模块的 APP 处理,再将结果送往 USIM 卡,用外部输出编码处理,最后将加密/解密结果回传给 APP. 这种模式使得该白盒密码模块只能在插了配套的 USIM 卡的手机中正常使用.

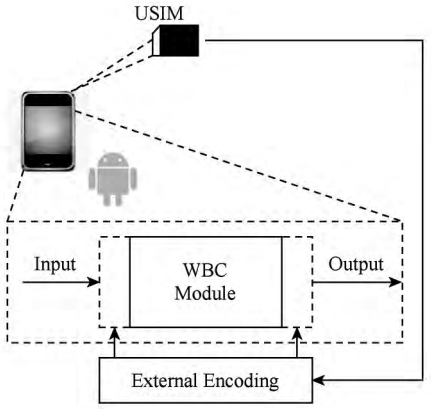

Fig. 4　The application of white-box cryptography in a smart phone.

图 4　白盒密码在智能手机中的应用

除了用硬件技术保护外部编码,还有用软件技术保护的方法,例如安全隔离区等[14]. 本文采用前者,根据输入参数和内置的根密钥在芯片内派生外部编码,提出了基于白盒密码的 DCAS 终端安全芯片改进方案. 由于体积和运行效率的限制,白盒密码模块适合在密钥更新不频繁以及加/解密数据量不大的情况下使用. 由于业务密钥 SK 一般是 1 个月

1 换，并且仅用来解密密文形式的控制字 $E_{SK}(CW)$，所以我们拟用白盒密码来完成这个解密操作.

3 基于白盒密码的 DCAS 安全芯片方案

3.1 安全芯片的功能

我们的终端安全芯片如图 5 所示，功能包括：OTP、外部编码派生和解扰及解码等模块. 层级密钥的功能由应用软件中的白盒密码模块(简记为 $WBCM$)以及安全芯片内的外部编码配合完成. 与图 4 稍有不同，在我们的方案中，白盒密码模块的输入端没有使用外部编码，仅在输出端使用受黑盒保护的外部输出编码(简记为 $ExtEnc$)，达到将 $WBCM$ 与终端硬件捆绑的目的即可. 用户终端收到 $E_{SK}(CW)$ 后，解密操作由 $ExtEnc \circ WBCM$ 完成.

安全芯片的工作流程如下：芯片上电后，OTP 用还原函数将内置的 $ESCK$ 还原成 SCK，并提供给外部编码派生模块，用于生成 $ExtEnc$；如果终端本地没有 $WBCM$ 或者 $WBCM$ 需要更新，终端从前端服务器下载 $WBCM$；$WBCM$ 和 $ExtEnc$ 配合完成 CW 的解密以及握手认证流程；最终解密得到的 CW 被送至解扰及解码模块.

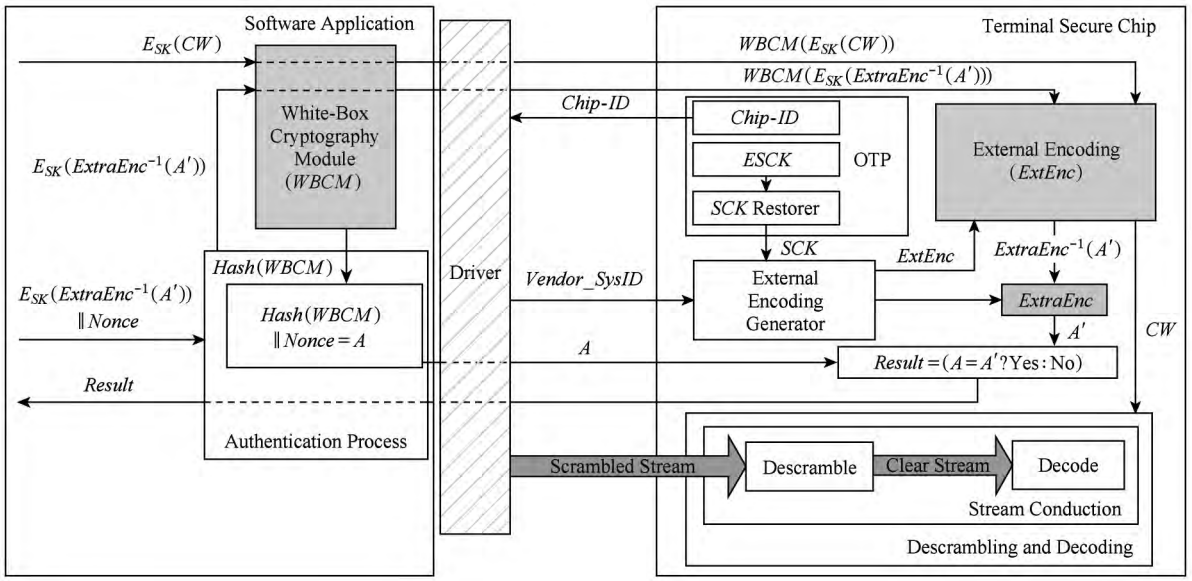

Fig. 5 A white-box-cryptography-based scheme for the secure chip of DCAS terminal.

图 5 基于白盒密码的 DCAS 终端安全芯片方案

外部编码派生模块根据输入的服务商系统标识 $Vendor\_SysID$ 及芯片内的 SCK，派生出外部编码. 不同的服务商可生成不同的外部编码. 即便是同一家服务商，也可以定期在一定范围内变动 $Vendor\_SysID$，以获得更大的安全性.

3.2 密钥的更新及解密流程

$WBCM$ 的体积较大，而且每个终端需要的 $WBCM$ 都不同，所以 $WBCM$ 不适合在传输流中广播发送. 本文的方案面向双向网络. EMM 流中循环广播的不是加密后的密钥，而是每个 DCAS 用户终端下载 $WBCM$ 时使用的链接. 终端发现本地的 $WBCM$ 过期或者收到前端服务器发送的更新通知后，使用标识身份的 $Chip\text{-}ID$ 从 EMM 中检索出 $WBCM$ 的下载链接，然后向前端服务器请求下载.

前端服务器在每次收到下载请求时，实时生成 $WBCM$ 并返回给终端，服务器仅保留 $WBCM$ 的散列值. 由于 $WBCM$ 由查找表网络构成，表与表之间的编码是随机选择并相互抵消的，所以我们可以注意到这样的事实，即：将 $WBCM$ 视作 2 进制文件，即使是同一个终端和相同的 SK，终端每次请求到的结果也是不一样的，其散列值也会不同(发生碰撞的概率由选择的散列算法决定).

DCAS 终端的解密流程为

1) 软件应用接收密文 $E_{SK}(CW)$，使用 $WBCM$ 部分解密，得到 $WBCM(E_{SK}(CW))$，发送给安全芯片；

2) 安全芯片接收到 $WBCM(E_{SK}(CW))$ 后，使用 $ExtEnc$ 解密，得到 CW，即：

$$CW = ExtEnc(WBCM(E_{SK}(CW))) = D_{SK}(E_{SK}(CW)).$$

这样的流程相当于用 2 层密钥加密 CW. 每个节目流中的 ECM 与前述 CAS 安全原理中的保持一致. 由于方案是面向双向网络，用户向前端服务器主动请求属于自己的密钥，所以不需要用多层加密来减少 EMM 中循环广播的数据量. $WBCM$ 中实现

的算法可以选用 AES,TDES,SMS4 等已有白盒密码实现的算法,或者其他新设计的白盒密码.

3.3　一种外部编码生成算法

目前常见的安全芯片内的 RAM 和 ROM 都仅有几十 KB,如果外部编码的生成算法太复杂或者生成的外部编码占用太大存储空间,该算法就不能在安全芯片中使用.本节设计一种适合在安全芯片内实现的外部编码生成算法.生成的外部编码结构如图 6 所示(以每次处理 128 b 的分组为例),包含 32 个 4 b→4 b 的非线性双射 $F_i, i=0,1,\cdots,31$ 和 1 个 32 b→32 b 的线性双射 G. F_i 是根据参数生成的,而 G 是 1 个具有良好扩散性质的常量.

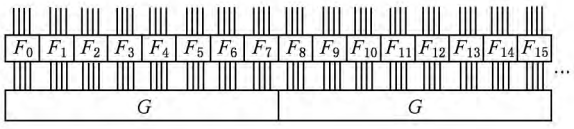

Fig. 6　Structure of a 128 b→128 b external encoding.

图 6　128 b→128 b 的外部编码结构

F_i 的生成如图 7 所示.伪随机数生成器(pseudo-random number generator, PRNG)根据输入的种子参数 $Vendor\_SysID \| SCK$ 生成比特流,其中 ‖ 代表 2 个参数的串联.比特流中每 64 b 可以用来生成 1 个 F_i.算法 1 描述了详细过程.

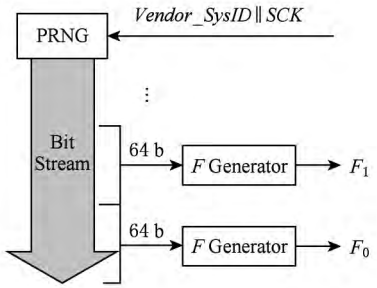

Fig. 7　Generation of $F_i, i=0,1,\cdots,31$.

图 7　F_i 的生成,$i=0,1,\cdots,31$

设有序整数集合 $GP=\{i \mid i=0,1,\cdots,15\}$,其中的元素按从小到大的顺序排列.1 个 4 b→4 b 的非线性双射 F 可被视为 1 个 $GP\rightarrow GP$ 的双射.

算法 1. 4 b→4 b 非线性双射的生成算法.

目标:生成 $GP\rightarrow GP$ 的双射 F;

输入:整数数组 $PRN[16]$,$PRN[16]$用从伪随机数生成器得到的 64 b 数据初始化,将每 4 b 的数据视为 1 个 0～15 的 10 进制数,数组的 16 个元素依次装载 4 b;

输出:整数数组 $F[16]$,$F[i]$代表 i 经过双射 F 作用后的数值,i 和 $F[i]$都属于 $GP, i=0,1,\cdots,15$;

变量:整数 $range$ 初始化为 16,有序整数集合 GP_T 初始化为 GP,整数 $index$ 初始化为 0.

步骤 1. $PRN[index]=PRN[index] \bmod range$, $F[index]=GP\_T[PRN[index]]$;

步骤 2. 将 $GP_T[PRN[index]]$从 GP_T 中删除,GP_T 重新排序,$range$ 减 1,$index$ 加 1;

步骤 3. 如果 $range>0$,则返回步骤 1;

步骤 4. 得到数组 $F[16]$,此时集合 $GP\_T=\varnothing$.

算法 1 生成的结果可以用 1 个 16 行、每行 4 b 数据的查找表存储,将占用 8 B 的存储空间.32 个非线性双射共占用存储空间 256 B.

外部编码的使用流程为:输入的 128 b 数据先以每 4 b 为 1 组用 F_i 处理,将处理后的 128 b 数据再以每 32 b 为 1 组用 G 处理.由于攻击者看不到安全芯片内的 F_i,所以 F_i 和 G 不用像之前叙述的编码一样合成在一起.

G 是线性变换,为了提高运算速度,G 可以用 4 个 8 b→32 b 的查找表实现,共占用 4 KB 的存储空间.加上非线性编码,整个外部编码占用的存储空间不超过 5 KB,是完全能够用目前的安全芯片技术实现的.

我们用 AES 算法中的列混合矩阵作为 G 以及用 RC4 算法作为伪随机数生成器,验证本节介绍的外部编码生成算法的正确性,即生成的外部编码 $ExtEnc$ 是 1 个伪随机的双射.举例假设输入的分组数据 $Input$,$Vender\_SysID$,SCK 分别是 16 B,8 B,16 B 的数据(用 16 进制表示),验证结果如下:

1) 取:

$Vendor\_SysID$=a35f425b0b4cd971,

SCK=1c32d8e9f46a7e85b67f04d9a0732b48,

以 $Vendor\_SysID \| SCK$ 作为 RC4 的种子密钥,由算法 1 生成 $ExtEnc$;

2) 取:

$Input$=c56a809bd706e54f367e97a1540b32a5,

经 $ExtEnc$ 作用后得到输出:

$Output$=99daa7256a1e561b90d26c1b23dbde3;

3) 经验证,2)中的 $Output$ 用 $ExtEnc$ 的逆映射作用后能够还原为 $Input$.

3.4　外部编码的安全性

DCAS 终端安全芯片内是受保护的运行环境,其中的外部编码可以被看作是 1 个运行在黑盒中的分组密码.密文输入后,在芯片内部用外部编码解密.根据使用方式的不同,攻击者可以对外部编码进行被动/主动攻击.

如果解密后的数据直接输出安全芯片外，攻击者则可以通过控制安全芯片的输入得到任意密明文对，进行选择明文攻击，这是一种很强的主动攻击. 受安全芯片的计算资源限制，本文方案中的 $ExtEnc$ 结构很简单，其中的扩散矩阵还是固定和公开的，所以如果攻击者进行差分攻击，$ExtEnc$ 很快会被破解.

为了避免 $ExtEnc$ 遭受主动攻击，安全芯片应该将解密后的内容留在芯片内使用. 在本方案中，解密后的 CW 被直接送往芯片内的解扰和解码模块，攻击者无法观察到. 从 CW 的解密流程来看，攻击者只能对 $ExtEnc$ 进行唯密文攻击. 如果对 32 个非线性双射进行唯密文的穷举攻击，需要尝试的最大次数为：$(16!)^{32}\approx 2^{1416}$，即平均需尝试 2^{1415} 次，远大于穷举芯片内根密钥的尝试次数，所以方案是安全的.

3.5 基于零知识证明的握手认证

从 3.4 节的安全性讨论中，我们知道安全芯片不能将外部编码处理后的消息直接送出芯片外，所以本方案中的握手认证是基于零知识证明的，以期将攻击者对外部编码的攻击控制在被动攻击的范围. 为了增强安全性，芯片内部增加 1 个 $ExtraEnc$ 输出编码，由 32 个 4 b→4 b 的非线性双射串联构成，其生成过程与外部编码中的类似.

握手认证的时序图如图 8 所示，其流程为

1) DCAS 终端的软件层接收从前端服务器发来的 $E_{SK}(ExtraEnc^{-1}(A'))\parallel Nonce$，其中，$A'$ 是 1 个挑战值，$Nonce$ 是 1 个随机数；

2) 软件层将消息用白盒密码模块处理后，将结果 $WBCM(E_{SK}(ExtraEnc^{-1}(A')))$ 发送给安全芯片；

3) 安全芯片计算出 A'：

$$ExtraEnc(ExtEnc(WBCM(E_{SK}(ExtraEnc^{-1}(A')))))=$$
$$ExtraEnc(D_{SK}(E_{SK}(ExtraEnc^{-1}(A'))))=$$
$$ExtraEnc(ExtraEnc^{-1}(A'))=$$
$$A';$$

4) 软件层计算 $A=Hash(WBCM)\parallel Nonce$，并传递给安全芯片；

5) 安全芯片比较 A 与 A' 是否相等，如果相等则返回 $Result=$Yes，反之返回 $Result=$No，软件层将收到的 $Result$ 作为对前端服务器的响应；

6) 重复 1)～5) 的过程 N 次，如果前端服务器 N 次都得到了正确的结果，则握手认证通过.

从握手认证的流程来看，攻击者无法利用安全芯片的输入和输出对外部编码进行主动攻击. 他可以通过观察，在安全芯片返回 Yes 时，收集到 1 个密明文对. 利用积累的密明文对，攻击者可以进行已知明文攻击. 因为握手验证过程并不频繁，所以积累密明文对是一个长期的观察过程，并且最后的攻击仍可能是穷举攻击. 已知明文下的穷举攻击需要尝试的最大次数为：$4\times(16!)^{16}\approx 2^{710}$，即平均需尝试 2^{709} 次，远大于穷举安全芯片内根密钥的尝试次数.

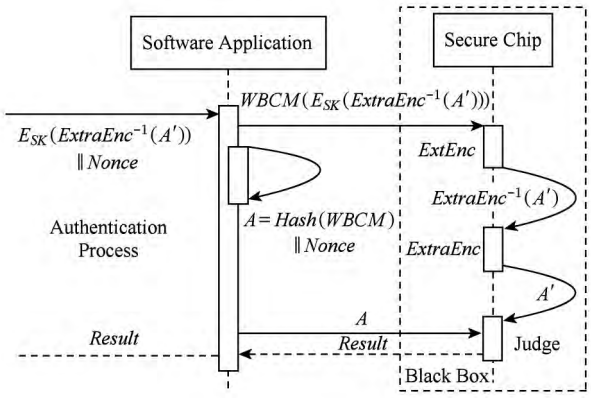

Fig. 8 Authentication process.

图 8 认证流程

我们的握手认证流程可以验证 DCAS 终端是否拥有解密 CW 的能力. 因为握手消息中加入了 $Hash(WBCM)$，我们还希望这个握手认证能够验证 DCAS 终端芯片在网络中的唯一性. 从 3.2 节我们知道，即使几个 DCAS 终端的安全芯片完全一样，下载到的 $WBCM$ 也不同，只有最后一次请求下载 $WBCM$ 的终端才能通过验证. 我们的认证流程使前端服务器可以侦测到被复制的芯片引起的异动. 一旦有异常就停止该芯片 $Chip\text{-}ID$ 对应的 $WBCM$ 的下载.

前端服务器可以取 A' 的值等于 A 或者不等于 A. 如果 $A'=A$，服务器预期终端的回答是 Yes，反之则是 No. 如果攻击者在软件层作为中间人，因为他无法知道 A'，只能向服务器返回猜测的 $Result$. 假设 $N=10$，他通过验证的概率仅仅是 $\frac{1}{2^{10}}\approx 0.0001$，即他几乎不可能用这种方法让非法终端通过验证.

当然，复制的终端可能利用合法的终端进行验证，即当复制的终端收到握手消息后，转发求助于合法终端. 这种攻击模式在终端被大规模复制的情况下很难实现；而小规模的复制，攻击者的成本太高，得不偿失. 所以我们的握手认证流程仍具有侦测异常，避免大规模损失的作用.

4　优缺点分析

与《DCAS 技术规范》中的方案相比,本文的改进具有 3 个优点:

1) 密钥和解密算法都包含在 *WBCM* 中,是一体的,终端通过前端服务器更新本地的 *WBCM* 时,可以一并更换.如果最坏的情况出现,攻击者同时拿到了 *WBCM* 和外部编码,由于模块体积和散列值的限制,在使用时也不方便,他需要进一步破解出密钥.

2) 芯片里的黑盒内容减少,增加了芯片在使用时的灵活性和通用性,还有利于控制芯片成本.安全芯片内不可能容纳所有密码算法,将密码算法在芯片外用软件实现,又能保证安全性,这正是白盒密码的价值.

3) 改进后的握手验证过程在判断 DCAS 终端可用性的同时,还可以验证终端的唯一性,可以监测出 DCAS 终端被复制或者被大规模复制的情况.

本文方案的缺点:《DCAS 技术规范》中的方案兼容单向广播网络的 CAS,而本文的方案是面向双向网络的,不能兼容旧系统是本文方案的最大缺点.

5　结束语

本文将《DCAS 技术规范》中的终端安全芯片作为研究对象,为了得到更加灵活通用、成本更低的安全芯片,提出了一种基于白盒密码的解决方案.本文的方案为以后 DCAS 技术规范的更新拓展了思路.本文提出在硬件黑盒中根据输入参数生成外部编码绑定黑盒外的白盒密码软件模块的方法,也可以在其他场景中使用.如何根据不同应用环境的需求设计更高效安全的外部编码生成算法以及分析白盒密码的安全性是有待进一步研究的课题.

参　考　文　献

[1] SARFT of the PRC. GY/T 255—2012 Technical Specification of Downloadable Conditional Access System [S]. Beijing: Academy of Broadcasting Planning, SARFT of the PRC, 2012 (in Chinese)
(国家广播电影电视总局. GY/T 255—2012 可下载条件接收系统技术规范[S]. 北京:国家广播电影电视总局广播电视规划院,2012)

[2] Chow S, Eisen P, Johnson H, et al. White-box cryptography and an AES implementation [G] //LNCS 2595: Selected Areas in Cryptography (SAC 2002). Berlin: Springer, 2003: 250-270

[3] ITU Rec. 810, Conditional-Access Broadcasting Systems [S]. Geneva, Switzerland: ITU-R, 1992

[4] ETSI. EN 300 744 V1.6.1 Digital Video Broadcasting (DVB); Framing Structure, Channel Coding and Modulation for Digital Terrestrial Television [S]. Sophia Antipolis, FRA: ETSI, 2009

[5] Chow S, Eisen P, Johnson H, et al. A white-box DES implementation for DRM applications [G] //LNCS 2696: Digital Rights Management (DRM 2002). Berlin: Springer, 2003: 1-15

[6] Jacob M, Boneh D, Felten E. Attacking an obfuscated cipher by injecting faults [G] //LNCS 2696: Digital Rights Management (DRM 2002). Berlin: Springer, 2003: 16-31

[7] Billet O, Gilbert H, Ech-Chatbi C. Cryptanalysis of a white box AES implementation [G] //LNCS 3357: Selected Areas in Cryptography (SAC 2004). Berlin: Springer, 2005: 227-240

[8] Goubin L, Masereel J M, Quisquater M. Cryptanalysis of white box DES implementations [G] //LNCS 4876: Selected Areas in Cryptography (SAC 2007). Berlin: Springer, 2007: 278-295

[9] Lepoint T, Rivain M, De Mulder Y, et al. Two attacks on a white-box AES implementation [G] //LNCS 8282: Selected Areas in Cryptography (SAC 2013). Berlin: Springer, 2014: 265-285

[10] Xiao Y, Lai X. A secure implementation of white-box AES [C] //Proc of the 2nd Int Conf on Computer Science and Its Applications. Piscataway, NJ: IEEE, 2009: 1-6

[11] Karroumi M. Protecting white-box AES with dual ciphers [G] //LNCS 6476: Information Security and Cryptology (ICISC 2010). Berlin: Springer, 2011: 278-291

[12] De Mulder Y, Roelse P, Preneel B. Cryptanalysis of the Xiao-Lai white-box AES implementation [G] //LNCS 7707: Selected Areas in Cryptography (SAC 2012). Berlin: Springer, 2013: 34-49

[13] Michiels W, Gorissen P, Hollmann H D L. Cryptanalysis of a generic class of white-box implementations [G] //LNCS 5381: Selected Areas in Cryptography (SAC 2008). Berlin: Springer, 2009: 414-428

[14] Park J Y, Kim J N, Lim J D, et al. A whitebox cryptography application for mobile device security against whitebox attacks-How to apply WBC on mobile device [C] // Proc of the 4th Int Conf on IT Convergence and Security. Piscataway, NJ: IEEE, 2014: 1-5

Xu Tao, born in 1977. PhD candidate. His main research interests include white-box cryptography and IoT security.

Wu Chuankun, born in 1964. Professor and PhD supervisor at the Institute of Information Engineering, Chinese Academy of Sciences. His main research interests include network security protocols, white-box cryptography and IoT security.

Zhang Weiming, born in 1976. Associate professor and master supervisor in the University of Science and Technology of China. His main research interests include information hiding and network security (zhangwm@ustc.edu.cn).

《计算机研究与发展》征订启事

《计算机研究与发展》(Journal of Computer Research and Development)是中国科学院计算技术研究所和中国计算机学会联合主办、科学出版社出版的学术性刊物,中国计算机学会会刊.主要刊登计算机科学技术领域高水平的学术论文、最新科研成果和重大应用成果.读者对象为从事计算机研究与开发的研究人员、工程技术人员、各大专院校计算机相关专业的师生以及高新企业研发人员等.

《计算机研究与发展》于1958年创刊,是我国第一个计算机刊物,现已成为我国计算机领域权威性的学术期刊之一.并历次被评为我国计算机类核心期刊,多次被评为"中国百种杰出学术期刊".此外,还被《中国学术期刊文摘》、《中国科学引文索引》、"中国科学引文数据库"、"中国科技论文统计源数据库"、美国工程索引(Ei)检索系统、日本《科学技术文献速报》、俄罗斯《文摘杂志》、英国《科学文摘》(SA)等国内外重要检索机构收录.

国内邮发代号:2-654;**国外发行代号**:M603

国内统一连续出版物号:CN11-1777/TP

国际标准连续出版物号:ISSN1000-1239

联系方式:

100190 **北京中关村科学院南路6号《计算机研究与发展》编辑部**

电话:+86(10)62620696(**兼传真**);+86(10)62600350

Email:crad@ict.ac.cn

http://crad.ict.ac.cn