

白盒密码研究*

林婷婷, 来学嘉

上海交通大学 计算机科学与工程系 密码与信息安全研究所, 上海 200240

通讯作者: 来学嘉, E-mail: lai-xj@cs.sjtu.edu.cn

摘要: 传统密码学原语的安全性基于黑盒攻击模型, 在这个模型中, 攻击者只能对密码学原语进行黑盒访问(即“随机预言”访问), 而对程序运行时的内部状态一无所知. 理论上讲, 不考虑现实生活中程序运行时各种类型的信息泄露的话, 这样的假设是合理的. 但实际上, 一旦我们在终端运行程序时, 总会发生各种信息的泄露, 造成更强的攻击. 白盒攻击即是这样的一种攻击, 它有别于传统密码模型中定义的攻击类型, 它假设攻击者对设备终端(即应用程序的运行环境)拥有完全的控制能力, 能够观测并更改软件运行时的所有内部数据, 攻击者具有更强的攻击能力. 因此, 传统黑盒模型下安全的密码学原语在白盒攻击模型下极度的脆弱, 我们需要更高强度的密码体制来抵抗这种攻击. 本文介绍了白盒密码的起源及相关概念, 从基础理论研究和密码方案设计技术两方面总结归纳了其研究现状及发展动态, 并从效率 and 安全性上对目前已公开的白盒密码方案进行了评价. 最后, 对白盒密码的应用场景和有待解决的问题进行了说明.

关键词: 白盒密码; 混淆; 黑盒; 白盒实现; 软件保护

中图法分类号: TP309.7 文献标识码: A DOI: 10.13868/j.cnki.jcr.000077

中文引用格式: 林婷婷, 来学嘉. 白盒密码研究[J]. 密码学报, 2015, 2(3): 258-267.

英文引用格式: Lin T T, Lai X J. Research on white-box cryptography[J]. Journal of Cryptologic Research, 2015, 2(3): 258-267.

Research on White-box Cryptography

LIN Ting-Ting, LAI Xue-Jia

Institute of Cryptology and Information Security, Department of Computer Science & Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: LAI Xue-Jia, E-mail: lai-xj@cs.sjtu.edu.cn

Abstract: The security of traditional cryptographic primitive is based on the black-box attack model, in this model, an adversary is given black-box (oracle) access to the functionality and has no idea about the implementation details of the software. In theory, this model is rational if we ignore the information leakage from implementations in the real-world. However, once a cryptosystem is implemented in software, information leakage always happens and will result in stronger attacks. White-box attack is one of such attacks. It is different with attacks defined in traditional cryptography, it assumes that the adversary has full control over the execution

* 基金项目: 国家自然科学基金(61272440, 61472251); 中国博士后科学基金(2014T70417, 2013M531174); 保密通信重点实验室资助项目

收稿日期: 2015-04-21 定稿日期: 2015-05-06

environment of application programs and has total visibility of the internal values of the software. Adversaries in white-box attack context are much stronger than in black-box attack context, therefore, traditional cryptographic primitives are fragile, secure cryptosystems are needed to resist such attacks. This paper introduces the original idea and related notions of white-box cryptography, concludes the research status and development trends of white-box basic theories and design techniques, and evaluates efficiency and security for the public white-box cryptographic schemes. Also, this paper presents the application prospects of white-box cryptography and some unresolved issues.

Key words: white-box cryptography; obfuscation; black-box; white-box implementation; software-protection

1 引言

随着科学技术的快速发展, 电脑、互联网、智能手机等电子设备已经随处可见, 电视、电影、音乐、图片等数字化信息的广泛传播, 智能卡、移动令牌、无线传感器网络等设备的大量使用, 使得人们对秘密信息访问的途径越来越多, 从而密码算法的使用环境也不再单纯和可信. 例如, 用户在自己的机器上运行一个数字媒体的播放软件, 这个软件对加密过的数字信息进行解密后播放, 那么这些软件的运行环境很有可能是不安全的, 因为软件的解密过程对于攻击者(甚至可能就是用户本身)是可见的, 他们可以很容易就获得密钥信息; 同样, 无线传感器网络节点等通常配置在无人监管的场所, 因此, 对这些节点内部运行的观测、改动等都是有效的攻击手段. 所以, 针对运行终端的攻击非常的直接, 我们将这样的攻击称为白盒攻击.

白盒攻击的概念最早由 Chow 等人在 2002 年^[1]提出, 这里的“白盒”与程序检测中的“白盒测试”所指的环境有相通之处, 在白盒攻击中, 攻击者对设备终端(即应用程序的运行的环境)拥有完全的控制能力、与软件的执行者拥有同等的权利. 他可以对程序运行的二进制追踪、读取内存中的密钥、观察程序执行的中间结果、任意的静态分析以及改变子计算的结果等. 攻击者可以在终端做任何的操作, 相比传统的黑盒模型, 对攻击者的能力只有很少的限制.

白盒攻击是在不可信任终端环境下产生的更高级的安全威胁. 白盒攻击可以看作是 man-at-the-end 攻击, 目前常见的直接白盒攻击有: OllyDbg、IDA Pro、HexRays、HIEW、VMware 等, 以及近年来提出的时间分析、功耗分析、插入错误分析等旁路攻击(side-channel attack)^[2-5]. 因此, 传统的密码算法在白盒攻击环境中不能安全使用, 显得极度脆弱. 所以, 为了保证在不可信任终端密码算法的加密、解密、认证等功能的正常使用, 构造出能够在白盒攻击环境下保证安全性的密码算法将是信息安全领域面临的一个重大课题.

我们将能够抵抗白盒攻击的密码算法及其实现称为白盒密码. 白盒密码包括了已有密码算法的白盒实现和白盒密码算法. 已有密码算法的白盒实现是指, 将已知的密码算法通过白盒密码技术进行设计, 使得在白盒攻击环境下, 不改变原算法的功能但原算法所希望保证的安全性不受破坏. 例如, 加密算法希望保证其密钥不会泄露、签名算法希望其签名不会被伪造等.

而白盒密码算法其实是指一种新的密码算法, 它与传统的密码算法不同的是, 它能够抵抗白盒攻击环境下敌手的攻击, 其本身是一个新的算法, 而不是在已存在的算法上的进行白盒安全实现的设计.

目前的白盒密码技术实例大部分为已知密码算法的白盒实现, 例如白盒 AES 实现^[1]、白盒 DES 实现^[6], 设计者们试图利用混淆的方式构造查找表, 并通过查表的方式来完成程序的执行, 使得白盒攻击者即使能够观察到整个查找表的查询, 也无法比穷举搜索更快地获得密钥信息, 以此抵抗白盒攻击. 但是事实证明这个方法的效果目前并不令人满意.

此外,也有设计者使用插入扰乱项^[7]或多变量密码^[8]的方式来提高攻击者的攻击难度,但是其安全性还有待商榷。除此之外,并没有公开的其他白盒密码的设计技术,但是信息隐藏、同态加密等方法也许可以应用到白盒密码的设计中来。

本文的结构如下安排:第2节介绍了白盒密码的起源及相关的三个概念:恶意主机攻击、旁信道攻击和混淆。第3节和第4节分别概括了白盒密码在理论方面和技术实现方面的一些最新研究进展,并对这些成果给出分析和评价。第5节介绍了白盒密码在实际中的应用和对密码学产生的影响。第6节我们对全文进行总结。

2 白盒密码的起源及相关概念

本节,我们将介绍三个不同的概念:恶意主机攻击、旁信道攻击和混淆,它们分别代表了白盒密码的起源、相似概念以及实现白盒密码的重要手段。

其中,恶意主机攻击可以看做是白盒密码研究的雏形;旁信道攻击与白盒攻击有部分相似,是近年来密码学上兴起的一种新型攻击,它对传统密码也具有巨大的威胁,但该攻击仍然包含在对白盒攻击的定义中;混淆的研究与白盒密码的研究相对独立地进行,但是在已有的白盒密码的设计中大量地使用了混淆的技术,两者之间具有密不可分的联系。

2.1 恶意主机攻击

恶意主机^[9,10]主要是指对那些在网络上自由漫游、可迁移到远程节点上执行以完成其所需任务的移动程序具有安全威胁的执行平台。恶意主机对移动程序产生安全威胁的最关键原因,在于主机对移动程序的执行具有完全的控制能力,因此,移动程序很难对主机隐藏秘密信息,它们可被恶意主机加以分析、修改、改变运行形态等。

目前恶意主机的研究,包括了认证^[11,12]、授权^[13]、黑洞搜索^[14]等,但是现有技术都无一例外地存在这样那样的问题,例如不能防范各种攻击、不适应开放的环境、灵活性不足、强度不够、涉及多信任域问题、对于轻量的移动代码计算强度过大等。因此,这一领域需要更多的研究与发展。

从白盒攻击的描述可以看出,两者之间具有很大的相似之处。但是事实上,他们并不完全相同。我们可以理解为白盒攻击环境是在恶意主机的基础上发展起来的,白盒攻击环境包含了恶意主机攻击。

2.2 旁信道攻击

1995年Paul在文献[15]中就提出了时差攻击,这个攻击根据不同密码学操作的时间差别来对密码系统的执行进行分析,从而获取秘密信息。这一类的物理攻击称之为“旁信道攻击”。类似的攻击还有很多,例如简单功耗分析(SPA),差分功耗分析(DPA),电磁分析(EMA)以及模版攻击^[16]等等。旁信道攻击模式也称为灰盒攻击模型(Grey-box attack model)。它与白盒攻击模型一样,也是针对密码算法执行时的安全性,它的某些攻击方式也可以在白盒攻击环境下使用。

两者的关系可以描述如下。

如果密码系统是白盒安全的,它在任何灰盒模型下也是安全的,因为密码算法执行操作所产生的物理上的泄露在白盒模型下是完全可见的。因此,安全的白盒密码不仅仅能抵抗目前已知的旁信道攻击,而且也能抵抗任何将来的旁信道攻击,可以说,未来白盒攻击可以取代旁信道攻击。

2.3 混淆

混淆就是将可执行程序转换成另外的不可理解的程序的过程,经过转换后的程序具有与原程序相同的功能,但运行该程序并不会泄露任何秘密信息,它可以保护程序在未知环境下正常运行,防止静态分

析、逆向工程和篡改等恶意攻击。尽管混淆与白盒密码各自独立地被提出进行研究,但它们具有紧密的联系。从某种意义上来说,白盒密码可看作是混淆技术在密码算法的程序实现上的应用;混淆技术是实现白盒密码的重要手段。

2000年, Hada 在文献[17]中第一次正式地研究代码混淆(code obfuscation), 而 Barak 等人^[18]在 2001 年提出了混淆的首个形式化定义, Canetti^[19]也针对点函数(point function)对混淆进行了正式的研究。一般地,混淆的定义如下:

定义 1 混淆器(Obfuscator) 一个概率算法 O 是一个混淆器, 如果满足以下三个条件:

- (1) 功能(Functionality)——任意的程序 p , $O(p)$ 描述了另一个程序, 在功能上与 p 相同。
- (2) 多项式效率(Polynomial slowdown)——存在多项式 P , 使得对任意的 $p: |O(p)| \leq P(p)$, 并且, 如果对于某些输入 x , 程序 p 在第 t 步终止, 那么 $O(p)$ 亦在 $P(t)$ 步终止。
- (3) 虚拟黑盒性(Virtual Black Box Property)——即使能够访问混淆程序 $O(p)$, 攻击者也不能够获得关于程序 p 的任何信息, 即不能从 p 的预言访问中获得任何信息。

对于混淆的应用, Barak 等人^[18]在他们的文献中指出, 不是所有的程序都是可以进行混淆的, 不可能构造出对所有程序族都通用的混淆器; 2005 年 Goldwasser 等人^[20]提出带辅助输入的虚拟黑盒混淆(virtual black-box obfuscation with auxiliary input)的概念, 同时也给出了关于混淆的负面结论; 2013 年, Bitansky 等人^[21]进一步证明了关于带辅助输入的虚拟黑盒混淆的否定结果。

但从正面的角度来看, Canetti^[19]在混淆的定义正式提出之前, 就已经在强的 DDH(Decisional Diffie-Hellman assumption)变体假设下, 提出了针对点函数族的混淆方法; 2004 年 Lynn 等人^[22]指出, 在随机预言机模型下, 点函数的混淆可以很简单地用一个随机预言机来实现; Wee^[23]在更强的假设下提出了一种点函数的混淆器; 其他学者^[24-27]也在各自对混淆的定义上给出了积极的结论。

混淆经过多年的研究已经取得了一系列的理论成果, 为白盒密码的研究提供了借鉴和学习的基础, 而白盒密码的发展也促进了混淆理论的发展。

除此之外, 白盒密码对算法的保护技术与同态函数(homomorphic functions)^[28-29]、不经意传输(oblivious transfer)^[30]也具有相似之处, 他们之间的关系有待进一步研究。

3 白盒密码理论方面研究进展

在基础理论方面, Chow 等人在 2002 年^[1]首先提出白盒攻击环境(White-Box Attack Context)的概念, 他假设:

- (1) 充分享有特权的攻击软件与密码学软件共享一个主机, 攻击软件对密码算法的执行完全可以访问。
- (2) 动态执行(与某个固定的密钥一起)是可以被观测的。
- (3) 密码算法的内部细节是完全可见和可任意更改的。

同时, 他们还给出了白盒多样性(white-box diversity)和白盒含混度(white-box ambiguity)两个概念来刻画白盒实现的安全性, 并说明他们的方案满足这两个白盒安全的要求。

在白盒密码的原语定义方面, Amitabh Saxena、Brecht Wyseur 等人^[31]在 2008 年给出了白盒性(White-box Property)的概念, 并且他们证明了其所谓的可能和不可能的结果((Im)possibility Results), 即证明了存在某些方案无法满足所有的白盒性, 也证明了存在某些方案, 在一定条件下可以满足某些白盒性。另外, Brecht Wyseur^[32]在白盒密码理论方面所做出的工作还体现在他 2009 年的博士论文中, 在他的这篇博

士论文中, Wyseur 对黑盒攻击、灰盒攻击和白盒攻击模型进行了比较, 对白盒密码学的目标和定义进行了描述.

除此之外, 2008 年, Herzberg 等人^[33]提出了白盒远程程序执行的概念(White-box Remote Program Execution), 并通过放松对 obfuscation 中函数的要求巧妙地避免了不可能的结论, 证明了在不可信任终端安全地执行程序是有可能的.

目前, 对于白盒密码基础理论的研究尚处于起步阶段, 对白盒安全性的测度问题除了 Chow 等人提出的白盒多样性(white-box diversity)和白盒含混度(white-box ambiguity)以外, 并没有再出现更好的测度方式. 因此, 对白盒密码进行建模和测度将是其理论基础研究未来的发展趋势.

4 白盒密码技术实现方面进展及其评价

目前常见的密码算法的白盒实现包括三种方式: Chow 等人^[1,6]的查找表方式、Bringer 等人^[7]的插入扰乱项的方式、Biryukov 等人^[8]的多变量密码的方式. 以下我们将逐一对三种方式以及其对应的实例进行归纳和总结.

4.1 查找表技术

4.1.1 Chow 的 AES 白盒实现

Chow 等设计的 AES 白盒实现^[1]的主要方法是给定一个密钥, 把 AES 的每一轮拆分成一个个小模块, 然后对每个小模块进行置乱编码, 并将每个模块所有可能的输入输出做成一个查找表, 用查找表来表示这些模块. 白盒 AES 的执行过程就转换成对一个个查找表进行查找的过程.

效率评价: 如上所述, 整个 AES 的执行过程都可以用查找表来实现, 每一次执行需要 3008 次查表. 总的查找表大小为 770048 B(752 KB).

安全评价: 在 2004 年, Billet 等人^[34]提出了一个非常有效的 BGE 攻击方法, 他们选择某些特定的查找表, 合并成一个可以用输入输出表示的函数, 使用代数的方法去掉其中的非线性部分, 提取出隐藏在 T-Box 中的密钥. 这个攻击在 2008 年由 Michiels 等人^[35]改进为一种通用攻击方法, 可以对类似算法的白盒实现进行攻击. 2013 年, Lepoint 等人^[36]提出了一种更加有效的攻击方法, 能够以 2^{22} 复杂度恢复 AES 的私钥.

4.1.2 Xiao-Lai 的 AES 白盒实现

Xiao-Lai^[37]的白盒 AES 实现是对 Chow 的白盒 AES 方案的一个改进, 其主要思想是: 改变 AES 原本一轮的边界, 把 AddRoundKey 和 SubBytes 组合在一起用 T-Box 表示, 对于固定的一个密钥计算出所有的 T-Box, 将 MixColumns 操作和 T-Box 合并到一个查找表中, 并将 ShiftRows 结合到输入输出置乱编码中. 此方案对文献[1]的改进在于在每一轮中将两个并行的查找表合成为一个查找表, 从而增加了 BGE 攻击的难度.

效率评价: Xiao-Lai 的 AES 白盒实现一共用到 80 个查找表, 40 次异或操作以及 11 个 128×128 的矩阵. 实现总共需要占用 $11 \times (128 \times 128) + 80 \times (2^{16} \times 32) + 120 = 20502 \text{KB}$.

安全评价: Xiao 等人从查找表的白盒多样性以及白盒含混度的角度进行分析, 说明了此方案足以抵抗暴力攻击. 此外, 由于此方案正是在 BGE 攻击的基础上对 Chow 的白盒 AES 的改进, 因此它能够抵抗类似 BGE 的攻击. 但是 2012 年, Mulder 等人^[38]使用 Biryukov 等人^[39]提出的线性/仿射等价算法(Linear and Affine Equivalence Algorithms)成功地提取密钥.

4.1.3 肖的 SMS4 白盒实现

2009年,肖雅莹和来学嘉^[40]在密码学年会上提出了 SMS4 算法的白盒实现,基本思想是将 SMS4 的每一轮中的某些步骤合成一个查找表,再利用可逆仿射变换作为输入编码(Input-Encoding)和输出编码(Output-Encoding)将其混淆,其方法与 Chow 等人的白盒 AES 相似。

效率评价: 每一轮的白盒 SMS4 需要 3 个部分,包括 5 个放射变化和 4 个查找表,因此所占有的空间为: $152192 \text{ B} = 148.625 \text{ KB}$ 。同时白盒 SMS4 每一轮跟标准 SMS4 算法相比较,多出了 5 个仿射变换,白盒 SMS4 算法的执行时间会比 SMS4 算法慢。

安全评价: 此 SMS4 的白盒实现在白盒多样性、白盒含混度和局部安全性上达到了一定的要求,文中也声称能抵抗类似 BGE 的攻击方法,而是否能抵抗其他的攻击则未见论述。但在 2013 年,林婷婷等人^[41]对其进行分析,以低于 2^{47} 的时间复杂度恢复出密钥。

4.1.4 Chow 的 DES 白盒实现

文献[6]的主要思想是将 DES 的每一轮分为非线性层(Cr)和仿射变换层(Dr)。非线性层主要是指 S 盒操作,仿射变换层包括移位、异或、扩展置换 E、置换 P 等。此方案采用与文献[1]相同的方法,不同之处在于对每个模块的划分不再局限于一轮以内,而是尽量模糊轮边界的方式来划分模块。这样可以在一定程度上增加攻击者的难度。

效率评价: 在白盒 DES 的实现中,会大量的使用到 96×96 矩阵的分块矩阵的运算,以及级联编码和异或。虽然对具体的执行步骤没有进行详细的统计,但是文中“本文我们大量地忽略空间和时间要求,仅仅关注……”,从侧面反映了本方案的效率。

安全评价: 虽然 Chow 声称在白盒环境下,此方案可以使得攻击者获取密钥变得困难,但此方案已陆续被多名学者攻破。2002 年, Jacob 等人^[42]指出,白盒实现方法并不安全,他们针对无外部编码(External Encoding)的 DES 白盒构造了一种“注入错误攻击”(Fault-Injection Attack),可以以较低的复杂度找出密钥。2005 年 Link 等人^[43]针对这个攻击对白盒 DES 的进行改进,并得出了一个新的 DES 白盒实现方案,这个方案在当时能抵抗已知的几个攻击。2007 年, Wyseur 等人^[44]在不考虑外部编码的情况下,基于内部信息,利用截断差分分析提出了一种攻击;同年, Goubin 等人^[45]也基于截断差分分析,针对白盒 DES 执行的第一轮提出了一种攻击。

4.2 插入扰乱项

4.2.1 Bringer 的 AES 白盒实现

与前面文献所使用的方法全然不同,2006 年 Bringer 等人在文献[7]中提出一个新 AES 白盒实现方法,该方法使用同构多项式问题(Isomorphism of Polynomials, IP problem)^[46],采用与文献[47]同样的技术,其主要思想是增加额外的扰乱方程到原始的方程中去,以此来扰乱原本方程中的代数结构,从而使得针对代数结构进行的攻击变得困难。

效率评价: Bringer 白盒 AES 实现一个实例需要占用 142 MB 空间,因为其方案中采用的 0 多项式由 4 个多项式来构造,需要 4 个运行实例,所以该白盒实现方法最后需要占用 568 MB 空间,其总共占用空间比 Chow 的白盒实现提高了近 900 倍。

安全评价: Bringer 等人在文中从三个方面对其方案的安全性进行了分析,说明该方案有足够的的能力抵抗其描述的攻击。但是,2010 年 Mulder 等人在文献[48]中提出对该白盒 AES 实现的攻击方法,能够以较低的复杂度恢复出等价密钥。

4.3 多变量密码的方式

在各种白盒实现方案被相继攻破之后, 2014年, Alex Biryukov 等人^[8]提出了一种新的白盒密码设计方式. 这种设计方式并不是已有的密码算法的白盒实现, 而是基于 ASASA(Affine-Sbox)结构的通用白盒密码设计.

Alex 等人的设计分为两类: 强白盒密码设计和弱白盒密码设计. 在强白盒密码中, 作者使用有限域上的多变量多项式的方法, 分别以 χ -scheme 和扩展 S 盒(expanding S-box)来实现 ASASA 中的 S 盒, 得出两种不同的 ASASA 白盒方案, 这两种方案都需要插入扰乱项来抵抗攻击.

在弱白盒密码中, 作者使用查找表的方式来实现. 第一种方案是单一 ASASA 结构的对称加密方案. 第二种方案是一个 SPN 结构的对称加密方案, 该方案 S(代换)层由多个第一种方案中构造的 ASASA 或单一的 S 盒构成, 每一个 ASASA 模块或 S 盒由一个查找表实现.

效率评价: 以 128 bit 输入为例, 在强白盒密码的两个方案中, 以 χ -scheme 构造非线性层的方案需要 300 MB 存储空间, 以扩展 S 盒来构造非线性层的方案需要 24 MB. 弱白盒密码的两个方案中, 单一 ASASA 结构的对称加密方案需要 196 KB, SPN 结构的对称加密方案按照不同层数最低需要 8 MB 的存储空间, 最高需要 20 GB 的存储空间.

安全评价: 目前, 除了文中作者的安全性分析以外, 还未有针对这四种方案的已知攻击.

5 白盒密码的应用

由上可以看出, 白盒密码是密码学理论研究的一个新方向, 它颠覆了传统密码学对攻击者能力的诸多限制, 更加符合实际生活中的安全威胁. 白盒密码及其特性无论在理论上还是实际应用中都具有重要的、广阔的应用前景, 将会对密码学产生巨大的影响.

- (1) 数字版权管理(Digital Rights Management, DRM)问题, 通过对播放软件的白盒加密, 白盒密码可以保证数字媒体只在经过付费授权的终端播放;
- (2) 云计算(Cloud computing)问题, 对云上的软件使用白盒密码, 可以保证在“云”这个不可信任终端上进行加解密运算时, 用户需要保密的信息不会被泄露.
- (3) 手机安全使用问题, 白盒密码能够保证, 手机即使被恶意使用者所掌控, 也不会泄露手机中固有的机密信息, 例如手机丢失后, 手机中保存的原使用者的银行支付密码.
- (4) 将私钥加密转换为公钥加密, 将一个私钥加密算法 E_k 的白盒实现构造为 $WB(E_k)$, 即为一个公钥加密方案. 任何人获得 $WB(E_k)$ 都可以加密消息, 而仅有知道私钥 k 的人才能利用解密算法 E_k^{-1} 进行解密. 注意: 这个转换需要 E_k 和 E_k^{-1} 不同, 同时应该也要保证 $WB(E_k)$ 保证通常意义下安全性, 例如单向性、语义安全等.

6 总结

白盒密码是一种高强度的密码算法, 因为它所面对的攻击者与传统密码学模型中的攻击者具有很大的不同, 他们具有目前所知道的最强攻击方式. 近十几年来, 密码学界对白盒密码的研究经历了从陌生到了解, 再到接受并主动研究的过程. 许多高校、研究所也积极地加入到了白盒密码的研究行列中来, 关于白盒密码的研究成果陆续出现在各种顶级会议和学术期刊上. 白盒密码已经成为了密码学最前沿的研究课题之一.

总的来说,在白盒密码的方案设计方面,虽然目前已经有一些白盒密码设计的突破进展,但其分析技术也出现了许多,因此迄今为止还未有能够得到公认的设计方法和方案,研究合理的白盒密码设计方法对于发展白盒密码来说是非常重要的一步.

同时,白盒密码基础理论的研究尚处于起步阶段,由于白盒密码攻击形式的特殊性,对其模型化与传统的密码学具有很大的不同,其安全性评价也没有统一的标准,因此对白盒密码进行建模和安全测度将是其理论基础研究未来的发展趋势.

References

- [1] Chow S, Eisen P, Johnson H, et al. White-box cryptography and an AES implementation[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2003: 250–270.
- [2] Anderson R, Kuhn M. Low cost attacks on tamper resistant devices[C]. In: Security Protocols. Springer Berlin Heidelberg, 1998: 125–136.
- [3] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems[C]. In: Advances in Cryptology—CRYPTO '97. Springer Berlin Heidelberg, 1997: 513–525.
- [4] Biham E, Shamir A. Power analysis of the key scheduling of the AES candidates[C]. In: Proceedings of the 2nd AES Candidate Conference. 1999: 115–121.
- [5] Boneh D, DeMillo R A, Lipton R J. On the importance of eliminating errors in cryptographic computations[J]. Journal of Cryptology, 2001, 14(2): 101–119.
- [6] Chow S, Eisen P, Johnson H, et al. A white-box DES implementation for DRM applications[C]. In: Digital Rights Management. Springer Berlin Heidelberg, 2003: 1–15.
- [7] Bringer J, Chabanne H, Dottax E. White box cryptography: another attempt[J]. IACR Cryptology ePrint Archive, 2006, 2006: 468.
- [8] Biryukov A, Bouillaguet C, Khovratovich D. Cryptographic schemes based on the ASASA structure: black-box, white-box, and public-key[C]. In: Advances in Cryptology—ASIACRYPT 2014. Springer Berlin Heidelberg, 2014: 63–84.
- [9] Hohl F. Time limited blackbox security: protecting mobile agents from malicious hosts[C]. In: Mobile Agents and Security. Springer Berlin Heidelberg, 1998: 92–113.
- [10] Sander T, Tschudin C F. Protecting mobile agents against malicious hosts[C]. In: Mobile Agents and Security. Springer Berlin Heidelberg, 1998: 44–60.
- [11] Kassab L L, Voas J. Agent trustworthiness[R]. In: NavalResearch Lab Washington DCCenter for High Assurance Computing Systems—CHACS, 1998.
- [12] Moon J S, Lee I Y, Yim K B, et al. An authentication and authorization protocol using ticket in pervasive environment[C]. In: 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops—WAINA. IEEE, 2010: 822–826.
- [13] Halonen T. Authentication and authorization in mobile environment[C]. In: Tik-110.501 Seminar on Network Security. 2000.
- [14] Dobrev S, Flocchini P, Kralovic R, et al. Black hole search by mobile agents in hypercubes and related networks[C]. In: OPODIS 2002. Springer Berlin Heidelberg, 2002: 169–180.
- [15] Kochev P C. BTiming attacks on implementations of Diffie-Hellman[C]. In: CRYPTO '96. Springer Berlin Heidelberg, 1996: 104–113.
- [16] Chari S, Rao J R, Rohatgi P. Template attacks[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2002. Springer Berlin Heidelberg, 2003: 13–28.
- [17] Hada S. Zero-knowledge and code obfuscation[C]. In: Advances in Cryptology—ASIACRYPT 2000. Springer Berlin Heidelberg, 2000: 443–457.
- [18] Barak B, Goldreich O, Impagliazzo R, et al. On the (im) possibility of obfuscating programs[C]. In: Advances in cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 1–18.
- [19] Canetti R. Towards realizing random oracles: Hash functions that hide all partial information[C]. In: Advances in Cryptology—CRYPTO '97. Springer Berlin Heidelberg, 1997: 455–469.
- [20] Goldwasser S, Kalai Y T. On the impossibility of obfuscation with auxiliary input[C]. In: 46th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2005. IEEE, 2005: 553–562.
- [21] Bitansky N, Canetti R, Paneth O, et al. More on the impossibility of virtual-black-box obfuscation with auxiliary input[J]. IACR Cryptology ePrint Archive, 2013, 2013: 701.

- [22] Lynn B, Prabhakaran M, Sahai A. Positive results and techniques for obfuscation[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 20–39.
- [23] Wee H. On obfuscating point functions[C]. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing. ACM, 2005: 523–532.
- [24] Hofheinz D, Malone-Lee J, Stam M. Obfuscation for cryptographic purposes[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2007: 214–232.
- [25] Canetti R, Dakdouk R R. Obfuscating point functions with multibit output[C]. In: Advances in Cryptology—EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 489–508.
- [26] Bitansky N, Canetti R. On strong simulation and composable point obfuscation[C]. In: Advances in Cryptology—CRYPTO 2010. Springer Berlin Heidelberg, 2010: 520–537.
- [27] Brakerski Z, Rothblum G N. Obfuscating conjunctions[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 416–434.
- [28] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 223–238.
- [29] Wyseur B, Deng M, Herlea T. A survey of homomorphic encryption schemes[R]. COSIC internal report, KatholiekeUniversiteit Leuven, 2007. 40.
- [30] Rabin M O. How to exchange secrets with oblivious transfer[J]. IACR Cryptology ePrint Archive, 2005, 2005: 187.
- [31] Saxena A, Wyseur B, Preneel B. Towards security notions for white-box cryptography[C]. In: Information Security. Springer Berlin Heidelberg, 2009: 49–58.
- [32] Wyseur B. White-Box Cryptography[D]. Doctoral thesis, KatholiekeUniversiteit Leuven, 2009.
- [33] Herzberg A, Shulman H, Saxena A, et al. Towards a theory of white-box security[C]. In: Emerging Challenges for Security, Privacy and Trust. Springer Berlin Heidelberg, 2009: 342–352.
- [34] Billet O, Gilbert H, Ech-Chatbi C. Cryptanalysis of a white box AES implementation[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2005: 227–240.
- [35] Michiels W, Gorissen P, Hollmann H D L. Cryptanalysis of a generic class of white-box implementations[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2009: 414–428.
- [36] Lepoint T, Rivain M. Another nail in the coffin of white-box AES implementations[J]. IACR Cryptology ePrint Archive, 2013, 2013: 455.
- [37] Xiao Y, Lai X. A secure implementation of white-box AES[C]. In: 2nd International Conference on Computer Science and its Applications, 2009. CSA 2009. IEEE, 2009: 1–6.
- [38] De Mulder Y, Roelse P, Preneel B. Cryptanalysis of the Xiao–Lai white-box AES implementation[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2013: 34–49.
- [39] Biryukov A, De Canniere C, Braeken A, et al. A toolbox for cryptanalysis: linear and affine equivalence algorithms[C]. In: Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003: 33–50.
- [40] Xiao Y Y, Lai X J. White-box cryptography and implementations of AES and SMS4[C]. In: ChinaCrypt2009. Science PressUSA Inc., 2009: 24–34.
肖雅莹, 来学嘉. 白盒密码及SMS4算法的白盒实现[C]. In: 中国密码学会2009年会. Science Press USA Inc., 2009: 24–34.
- [41] Lin T T, Lai X J. Efficient attack to white-box SMS4 implementation[J]. Journal of Software, 2013, 24(9): 2238–2249.
林婷婷, 来学嘉. 对白盒SMS4实现的一种有效攻击[J]. 软件学报, 2013, 24(9): 2238–2249.
- [42] Jacob M, Boneh D, Felten E. Attacking an obfuscated cipher by injecting faults[C]. In: Digital Rights Management. Springer Berlin Heidelberg, 2003: 16–31.
- [43] Link H E, Neumann W D. Clarifying obfuscation: improving the security of white-box DES[C]. International Conference on Information Technology: Coding and Computing—ITCC 2005. IEEE, 2005: 679–684.
- [44] Wyseur B, Michiels W, Gorissen P, et al. Cryptanalysis of white-box DES implementations with arbitrary external encodings[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2007: 264–277.
- [45] Goubin L, Masereel J M, Quisquater M. Cryptanalysis of white box DES implementations[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2007: 278–295.
- [46] Courtois N, Klimov A, Patarin J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]. In: Advances in Cryptology—EUROCRYPT 2000. Springer Berlin Heidelberg, 2000: 392–407.
- [47] Billet O, Gilbert H. A traceable block cipher[C]. In: Advances in Cryptology—ASIACRYPT 2003. Springer Berlin Heidelberg, 2003: 331–346.
- [48] De Mulder Y, Wyseur B, Preneel B. Cryptanalysis of a perturbed white-box AES implementation[C]. In: Progress in

Cryptology—INDOCRYPT 2010. Springer Berlin Heidelberg, 2010: 292–310.

- [49] Biryukov A, Bouillaguet C, Khovratovich D. Cryptographic schemes based on the ASASA structure: black-box, white-box, and public-key[C]. In: Advances in Cryptology—ASIACRYPT 2014. Springer Berlin Heidelberg, 2014: 63–84.

作者信息



林婷婷(1982–), 四川雅安人, 上海交通大学计算机科学与工程系博士研究生在读. 主要研究领域为密码算法设计与分析.
E-mail: lintingting00@163.com



来学嘉(1954–), 1992 年获得瑞士苏黎世高工技术科学博士学位, 教授、博士生导师. 与梅西教授共同设计 IDEA 加密算法, 被用于多个国际标准. 提出了用 DNA 技术的公钥密码算法及差分、高阶差分、马尔可夫密码的概念. 出版专著《分组密码的设计和安全性》, 并发表论文 100 多篇.
E-mail: lai-xj@cs.sjtu.edu.cn

2015 年安全协议进展国际会议通知

由中国密码学会安全协议专委会主办, 山东大学承办, 北京三未信安科技发展有限公司协办的“2015 年安全协议进展国际会议(2015 International Conference of Progress on Security Protocols, 简称 PSP 国际会议)”, 将于 2015 年 9 月 18 日至 20 日在山东省济南市召开.

会议旨在团结和吸引国内外安全协议领域的学者专家、行业精英、工程技术人员和在校研究生, 共同交流安全协议最新研究成果, 探讨安全协议研究领域最新成果和发展趋势, 提高学术研究水平并促进学术界和产业界的相互了解与合作. 届时将邀请 4–5 位密码学界知名专家作特邀报告.

热烈欢迎安全协议及相关领域科技人员和管理人员参加会议.

主办单位: 中国密码学会安全协议专业委员会

承办单位: 山东大学

会议时间: 2015 年 9 月 18–20 日

会议地点: 山东省济南市山大南路 27 号山东大学学人大厦

联系人: 刘 洁(财务), 010-59703688, 13661388568

杨晓燕(住宿预定), 15098865761

蒋 瀚(会议论文咨询), 18660749850

邮箱地址: xuqiuliang@sdu.edu.cn

会议网址: <http://isec.sdu.edu.cn/psp2015/>

中国密码学会安全协议专业委员会

2015 年 6 月 29 日