密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2016,3(6):527–545

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

流密码的设计与分析: 回顾、现状与展望*

张 斌, 徐 超, 冯登国

中国科学院软件研究所 计算机科学国家重点实验室, 可信计算与信息保障实验室, 北京 100190
通讯作者: 张斌, E-mail: zhangbin@tca.iscas.ac.cn

摘 要: 流密码的设计与分析一直都是密码学中的核心问题之一. 上世纪 40 年代, Shannon 证明了一次一密体制在唯密文攻击下在理论上的完善保密性, 激发了流密码研究的热潮, 自此流密码的设计都是围绕着如何产生接近完全随机的密钥流序列来进行, 发展出了基于线性反馈移位寄存器(LFSR)的若干设计范例, 许多基于此而设计的流密码纷纷被提出, 比如用于 GSM 通信安全的 A5/1 和蓝牙加密算法 E0 等, 同时也出现了像 RC4 等基于随机洗牌的设计范式. 在欧洲 NESSIE 和 eSTREAM 计划之后, 流密码的设计日趋多样化, 大量基于非线性反馈移位寄存器(NFSR)和基于分组密码扩散与混淆模块而设计的算法相继被提出, 以抵抗基于 LFSR 线性性质而发展的(快速)相关攻击与(快速)代数攻击等. 本文将首先回顾流密码设计与分析的发展历程, 系统地综述流密码设计与分析中的若干关键技术与方法, 同时介绍了目前最新的研究成果, 以及这个方向上目前需要解决的一些关键问题, 最后试着展望了一下未来流密码的发展方向.

关键词: 流密码; 流密码分析; 流密码设计
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000149

中文引用格式: 张斌, 徐超, 冯登国. 流密码的设计与分析: 回顾、现状与展望[J]. 密码学报, 2016, 3(6): 527–545.
英文引用格式: ZHANG B, XU C, FENG D G. Design and analysis of stream ciphers: past, present and future directions[J]. Journal of Cryptologic Research, 2016, 3(6): 527–545.

Design and Analysis of Stream Ciphers: Past, Present and Future Directions

ZHANG Bin, XU Chao, FENG Deng-Guo

TCA Lab, SKLCS, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
Corresponding author: ZHANG Bin, E-mail: zhangbin@tca.iscas.ac.cn

Abstract: As one of the most important problems in cryptography, the design and analysis of stream ciphers has always been a hot and central research topic. In the 40's of last century, Shannon proved in theory that the one-time pad cipher is secure in the ciphertext-only scenario, and triggered the fervor in stream ciphers. Since then, how to generate the keystreams which look like the purely random sequences as close as possible becomes the key point. As a result, many stream ciphers based on linear feedback shift registers (LFSR) are proposed, e.g., GSM A5/1 and Bluetooth encryption algorithm E0. At the same time, the design paradigm like RC4 based on random shuffles has also appeared. After the European NESSIE and eSTREAM projects, the design of stream ciphers gets more and more diversified. Many algorithms based on nonlinear feedback shift register (NFSR) and the confusion and diffusion principle in block ciphers have been proposed, which have good resistance against (fast) correlation and (fast) algebraic attacks. This paper first reviews the development history of the design and

* 基金项目: 国家自然科学基金项目(61572482); 国家重点基础研究发展项目(973 计划)(2013CB338002)
收稿日期: 2016-10-20 定稿日期: 2016-11-24

analysis of stream ciphers, and then reviews certain crucial technical methods with the latest research achievements, and some problems need to be solved in this direction. Finally, we try to foresee the future research directions in stream ciphers.

Key words: stream cipher; design of stream cipher; analysis of stream ciphers

1 引言

按照现代密码学的观点, 可以将密码体制分为对称密码体制和非对称密码体制; 对称加密算法又分为分组密码和流密码. 在分组密码中, 一般将消息分成固定长度的明文块来逐块进行加密; 而流密码则可较容易地实现任意长度消息的加密. 流密码使用一个时变函数来对每一个消息符号进行加密, 相比于分组密码, 流密码在理论和应用上具有一些无可比拟的优势.

流密码的实现非常简单, 便于软硬件实施, 同时流密码加密和解密的速度都很快, 没有或只有有限的错误传播. 这些特点使得流密码在实际中得到了广泛的应用, 特别是在政府、军事及外交部门, 流密码的应用几乎占据了主导地位. 1949 年 Shannon 证明了一次一密体制在唯密文攻击下是理论上不可破译、绝对安全的, 这可看成是最早的流密码方案; 然而, 为了建立一次一密的密码系统, 通常需要在安全信道上交换传输一个其长度至少和明文一样长的密钥, 这在很多情况下是不现实和不经济的, 在密钥的产生和管理方面也面临着许多复杂问题, 很容易造成各类安全隐患. 这也许就是后来人们设计各种流密码算法来代替一次一密体制的主要动因, 亦即各种流密码算法本质上都是对于一次一密体制的模仿, 同时消除了密钥产生、分配和管理维护中的各类问题; 流密码所产生的密钥流至少要做到看起来“很像”随机比特序列, 且恢复算法的初始状态和密钥、或者将算法及其密钥流与随机情况区分开来都是在一定计算能力与许可范围内困难的. 安全高效流密码的设计与分析一直都是密码学领域中核心研究方向与问题之一.

流密码一般可分为同步流密码和自同步流密码两大类. 在同步流密码中, 生成的密钥流和发送的明文消息之间相互独立, 其内部状态仅仅依赖于上一时刻的内部状态, 与输入明文无关. 同步流密码的优点在于其有限的错误传播, 当一个符号在传输过程中发生错误后不会影响到后续的符号. 而自同步流密码的密钥流则依赖于之前的明/密文信息, 常见的有类似于分组算法密文反馈模式的自同步流密码, 即密文参与密钥流的生成过程, 这使得这类流密码的安全性从理论上分析起来非常困难, 也造成这类算法的设计非常稀少. 目前常见的大多数流密码算法都是同步流密码, 因其设计上的可分析性, 使得设计者在设计过程中能够更好的理解自己所设计的流密码方案对于已知甚至某些未知攻击的抵抗力. 从总体上说, 一个流密码的安全性在很大程度上取决于其所采用的密钥流生成器, 由于以线性反馈移位寄存器为研究对象的伪随机序列代数理论的成熟, 上世纪 50、60 年代以来的大量流密码设计多是基于线性反馈移位寄存器(LFSR)而设计, 例如美国未公开的 Fibonacci 生成器、E0、A5/1 等. 另一方面, 由于 LFSR 的线性性质对于密码分析没有任何免疫力, 如 Berlekamp-Massey 算法等, 需要采用各种非线性部件来显式或隐式地掩盖线性性质与增强其非线性性, 常见的方法有非线性组合、非线性滤波、不规则钟控、带记忆及其各种组合方式等. 著名学者 Rueppel[1]给出了这一类流密码设计的一些方法和准则, 比如著名的线性驱动部件加非线性组合部件的设计范式. 这些代表了传统的流密码设计思路及其衍生准则, 其中一些已经很少见, 另外一些的影响则仍然存在.

现实中的情况在千禧年之始开始了变化. 2000 年, 欧洲提出了一个 NESSIE 计划(欧洲新签名、完整性和加密方案), 这个计划一直持续到 2003 年, 其目标之一就是征集新的流加密方案, 但很遗憾的是, 提交的所有流密码算法, 包括较为著名的 SNOW1.0, LILI-128[2]等, 在安全性方面都存在一些问题, 最终没有一个流密码能够入选. 虽然如此, NESSIE 计划激发了公开学者们对流密码研究的热情. 同年, 日本政府也提出了一个和 NESSIE 计划类似的项目, 称为 CRYPTREC, 其目的是征集和评估一些密码算法来用于政府和工业领域. 由此可见, 当时各界对于可靠安全的流密码设计方案是多么渴求, 这可以看作是对于 NIST 征集

AES 算法的一种反抗, 因为没有任何科学证据表明一个精心设计的流密码无法与 AES 算法相比; 恰恰相反, 相当多的学者认为流密码在某些应用环境下, 比如受限硬件环境和超高速软件加密时, 具有 AES 算法无法比拟的优点.

新世纪的伊始, 由于流密码代数攻击的提出, 传统的基于线性反馈移位寄存器的流密码设计方案进一步丧失了其吸引力. 为了进一步推动流密码的发展, 2004 年欧洲启动了 ECRYPT 计划, 其中就包含了专门面向流密码的 eSTREAM 计划, 其主要目标即是为了征集一些新的流密码算法, 以便于日后广泛的应用. eSTREAM 共征集到 34 个算法, 总体来看其设计非常多样化, 且大多数不再局限于传统的基于 LFSR 的结构, 而是采用了一些新的设计思路, 比如采用非线性反馈移位寄存器、采用类似分组密码的结构等. 具体来讲, eSTREAM 计划将流密码算法分为面向受限硬件环境的算法, 比如 eSTREAM 中的 Grain v1[3]、Trivium[4]、Mickey v2 等, 这些算法一般采用比特级的操作; 和面向高速软件应用的算法, 比如 Salsa20/12, SOSEMANUK, Rabbit, HC 等, 这些算法大都采用面向字的操作. eSTREAM 计划明显地影响了流密码的发展进程, 其后流密码的研究很快陷于沉静, 这主要是由于学术界对于大量采用极大内部状态和极高初始化轮数的新型流密码算法普遍缺乏有效的分析思想和办法, 这一状况也一直持续到今天. 期间虽有立方攻击、扩域上快速相关攻击等新方法的提出, 但对于采用极大内部状态和极高初始化轮数的流密码, 短时间内还是无法获得快于穷搜索的攻击方案. 在 ESC 2013 上, 一项新的对称加密体制竞赛项目被提出, 称为 CAESAR 计划, 其目的是征集认证加密算法, 传统的单一目的对称密码算法及其组合在某些情况下已经无法满足实际应用的需求, 在确保机密性的同时, 也要求保证信息的完整性, 这就是 CAESAR 竞赛的初衷. 从提交的算法和到目前为止的进程来看, 其主要思想仍然是 eSTREAM 计划最终入选算法的组合与改进, 唯一区别就是在传统的加密模块之外增加了认证模块, 及采用哈希函数结构而设计的流加密算法. 最近, 为满足同态加密应用环境的需求, 在 Eurocrypt 2016 上, 一个新的流密码结构被提出, 被称为置换滤波生成器, 这种结构可以看作是滤波生成器的一个变体, 以人为形式模拟产生大量的固定次数固定形式的代数等式.

在流密码分析方面, 根据 Kerckhoff 假设和攻击者所允许具有的信息与能力, 一般将分析方法分为下面 4 种:

(1) 唯密文攻击: 攻击者只知道密文信息.

(2) 已知明文攻击: 攻击者知道明文和相应的密文.

(3) 选择明文攻击: 攻击者可以根据需要选取一些明文, 并能够产生相应的密文.

(4) 选择密文攻击: 攻击者可以根据需要选取一些密文, 并能够获得相应的明文.

在一定密钥长度下, 相应地, 所谓流密码安全性也是相对于攻击类型和实际计算能力与代价而言的. 目前, 流密码分析方法主要有线性分析、相关分析、代数分析、时间存储折衷分析、猜测确定分析、初始化分析等. 现择要试言之. 最早的线性分析方法可以追溯到 CRYPTO 1989[5]和 CRYPTO 1990 上提出的线性校验子分析方法和和线性一致性分析方法, 但真正得到广泛应用的是 Matsui 对于 DES 的线性攻击方法, 即以线性操作代替非线性模块, 以概率意义下的相等代替通常的等式. 这是一种普遍适用的攻击思想, 具有非常强大的生命力. 由于流密码设计的多样性, 没有统一的路径来构造所分析体制的线性逼近, 这给予分析者极大困难的同时也带来了极大的机遇. 线性分析方法对于流密码的应用是一个随时间演变的进程, 困难且缓慢, 比较显著的结果如下. 在 CRYPTO 2002 上, Coppersmith[6]提出了 linear masking 思想, 其基本思路就是利用线性逼近建立关于密钥流和线性部分内部状态的一个关系, 然后利用线性反馈关系消去线性部分的内部状态, 从而建立一个只包含密钥流的线性逼近等式, 这个逼近等式和均匀分布相比较带有一定的概率偏差, 利用统计学原理, 即可以对密钥流和随机序列进行区分. 线性攻击的根本目的就是建立一个统计区分器, 通过区分两个不同的概率分布来获得流密码系统的一些弱点. 线性攻击的研究在对称密码学中一直都是非常主流的一个方向, 很多文献对线性攻击做了拓展和优化. 随着线性攻击的发展, 它被用来攻击许多流密码系统, 使得线性攻击也成为了流密码设计中必须考虑的基本攻击之一. 线性分析的理论

框架在分组密码中是比较成熟的, 而在流密码中却还有很多需要研究的方面, 对已有的流密码线性分析框架进行扩展和改进等在流密码的分析中是非常重要的研究课题.

作为另一种统计分析方法, 流密码相关攻击与线性分析相伴而生, 但更为有的放矢. 最早的相关攻击可追溯到非线性组合生成器的分析, 由相关性的"能量守恒定理"和我国著名密码学家肖国镇教授提出的Xiao-Massey 定理[7]知, 在这种流密码系统中, 输出序列总与一条或某一组 LFSRs 输出序列存在一定的相关性. 基于此, Siegenthaler[8]于 1985 年提出利用相关性, 可实现对于内部状态的分别征服, 从而大大降低寻找密钥所需的计算复杂度. 上世纪 90 年代, 一些学者给出了带记忆组合生成器相关特性的理论分析[9,10]. 对于基于 LFSR 的流密码, 通过各种不同的快速相关攻击[11−15]是一条经典的恢复出目标 LFSR 的内部状态的攻击路线. 再后来在文献[16,17]中, 相关性的定义被推广到条件相关性, 即在给定某些非线性函数的输出模式为条件下, 来研究输入变量之间的线性相关特性. 在 CRYPTO 2005[18]上, 一个对偶的、新的条件相关定义被给出, 即以某些位置输入作为条件来研究输出的线性相关. 这个方法随后被证明是分析带记忆流密码的一种重要手段, 通常情况下, 条件向量是和密钥相关的, 如果一个好的条件相关存在, 攻击者往往能够发现对应于正确密钥的样本序列是带有偏差的, 而错误密钥则近似于是随机样本序列. 相关攻击对带记忆流密码而言是一种非常有效的攻击方法, 通过寻找密码系统的有效线性逼近, 并结合编码理论可以有效地恢复密钥. 在 CRYPTO 2013 年, 我们[19]提出了一种更通用的条件相关攻击—条件掩码(condition masking)方法, 从而进一步拓展了条件相关攻击的适用范围. 时至今日, 相关攻击已发展成流密码分析方法中最为有效的一类分析手段, 是任何流密码算法在设计时都必须考虑的基本攻击之一.

相比于统计分析方法, 代数攻击是另一种对于基于 LFSR 流密码的典型攻击方法. 虽然代数攻击的思想可以追溯到 Shannon 的经典论述, 但直到 2003 年, Courtois 和 Meier 等人[20]才正式提出了流密码代数攻击的思想, 并对基于 LFSR 的流密码进行了代数分析, 将之应用到了 Toyocrypt 和 LILI-128 上. 在基于 LFSR 的流密码情形, 由于线性关系无法增加代数次数, 流密码的内部状态和密钥流比特通过非线性过滤函数或者组合函数直接组合, 缺乏动态增长, 易导致关于一定个数变量的大量固定次数代数关系式, 从而易被线性化方法恢复出初始状态变量. 如果非线性组合函数的代数次数比较低, 或者通过乘倍等化简技巧可以转化成代数次数较低的情况, 那么 LFSR 的初始状态可以通过线性化这些非线性方程所包含的单项式来恢复, 这亦是目前为止唯一可理论分析的代数攻击方法, 其他方法比如采用 Gröbner 基、XL、SAT 等, 虽然只需较少的密钥流即可攻击成功, 但缺乏对于流密码算法本身构造的有效利用, 只是现有解方程方法的直接使用, 从而难以获得广泛的关注和成功使用. 在 CRYPTO 2003 上, Courtois[21]进一步改进了代数攻击, 在获得连续密钥流的情况下, 提出了快速代数攻击的思想, 可以利用 Berlekamp-Massey 算法等方法, 局部地降低代数方程的次数, 从而减少单项式数目, 降低复杂度. 在一段时间内, 讨论代数攻击成为一种时尚, 各种改进方法纷纷被提出, 但有影响的方法不多, 具体可参看 Hellseth-Ronjom 等相关的工作; 但截至目前, 除了对于基于 LFSR 的流密码较为成功之外, 对于其他类型的密码体制的代数攻击则还有较长的路要走. 一般来说, 这里主要分为如何建立方程与如何求解方程两大步, 充分利用密码体制的特点来建立相对易解的方程组是一个十分重要的研究课题. 作为代数攻击的一个进展, 在 2009 年, 立方攻击被 Dinur 和 Shamir[22]提出, 其思想是利用高阶差分的性质来压缩原迭代函数, 在所获得的压缩结果是线性或者低次方程的情况下, 可以解方程获得初始密钥, 随后又有立方区分器, 动态立方攻击, 条件差分攻击等方法提出, 并被应用到 Trivium、Grain-128 和 Grain-128a 上, 其典型思想是利用可控制的 IV 变量来零化某些深度轮数的某些位置变量, 得到较易被区分的结果函数. 虽然看起来代数攻击是一种联系对称密码学与代数理论的天然桥梁, 但截至目前, 这种攻击方法还处在十分初始的阶段, 难以见到有影响力的工作.

时间存储数据折衷攻击(TMD)与猜测确定攻击一道, 可以看作是流密码体制的一种拓扑性质的分析, 即攻击者关注于流密码算法本身各个变量之间的依赖关系, 考察这些依赖关系是否导致其他攻击方法不易发现的漏洞. 目前关于时间存储数据折衷攻击已有较多的公开文献进行研究, 但对于猜测确定攻的研究还处于起步阶段, 只有较少的文献专门涉及这一问题. 具体来说, 时间存储数据折衷攻击由 Babbage[23]、

Golic、Biryukov 及 Shamir 等人提出, 从最初 Hellman 提出的对于 DES 的时间存储折衷攻击, 到目前一般性的逆向单向函数的方法, 折衷攻击作为一种方兴未艾的攻击思想还处在发展阶段. 目前存在多种关于时间存储数据折衷攻击的变形攻击, 较为成功的折衷攻击主要有对于 GSM 加密算法 A5/1 的时间存储数据折衷攻击, Rainbow 表方法等. 如果算法的内部状态较小, 就能够利用状态碰撞来恢复秘密信息; 如果算法的内部状态是密钥长度的至少两倍, 那么就需要根据一些折衷曲线来分析安全性了; 比较著名的折衷曲线是 2000 年 Biryukov 和 Shamir[4]提出的 $TM^2D^2 = N^2$ 等, 这里要注意的是预计算阶段的时间与存储复杂度不可忽略, 否则很容易导致片面的分析结果. 作为两种十分基础性的对称密码分析方法, 时间存储折衷攻击和猜测确定攻击在未来会发挥越来越大的作用.

另外一个值得深入研究的方向是根据算法特点, 来综合使用各种分析方法, 比如猜测确定攻击与相关攻击、代数攻击、时间存储折衷攻击的结合, 如果这种结合充分利用了算法本身的结构特点, 则往往能够构造出十分有威胁的攻击. 最后, 在某些特定环境下, 侧信道分析也是一种可考虑的攻击手段, 但本文暂不涉及各种侧信道攻击方法和应用.

本文的组织结构安排如下: 第 2 节主要回顾了流密码设计和分析的发展和现状. 第 3 节中给出流密码设计与分析中一些最新的研究成果. 第 4 节中指出目前流密码设计和分析所面临的一些问题, 以及未来的发展趋势和发展方向.

2 流密码设计和分析的发展和现状

在介绍流密码的设计与分析的一些关键技术之前, 我们先介绍流密码中常见的一些组件, 这些组件在设计算法以及分析算法中都起到了基础性的作用.

2.1 流密码常见组件

2.1.1 反馈移位寄存器

在流密码中最重要并且应用最广泛的是各类反馈移位寄存器, 最常见的反馈移位寄存器就是线性反馈移位寄存器(LFSR), 其结构如下图所示:

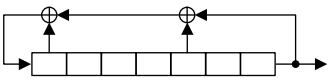

图 1 线性反馈移位寄存器

Figure 1 Linear feedback shift register

一个 LFSR 非常便于硬件实现, 在硬件上具有非常高的实现效率. LFSR 的输出可以表示成一个线性递归关系等式. 精心选择的 LFSR 会产生具有非常良好统计特性的序列; 但因其线性特性, LFSR 任意时刻的输出可以通过最初的内部状态线性推导表示出来.

定义 1(线性复杂度) 一个有限的二元序列的线性复杂度是指产生这段序列所需的最短 LFSR 的长度.

求一个有限序列的线性复杂度可以采用 Berlekamp-Massey 算法来快速计算, 计算长度为 $2n$ 的序列的线性复杂度所需的计算量最多为 n^2, 且往往可以改进为 $n \cdot \log n$.

另外一类在流密码中应用十分广泛的移位寄存器是非线性反馈移位寄存器(NFSR), 它的结构和 LFSR 类似, 但是其反馈函数不再是线性函数, 反而采用非线性布尔函数. 采用这一类组件的流密码算法有 Grain 系列算法、Trivium 等. 此外对于 NFSR 而言, 其 Fibonacci 和 Galois 表示之间也存在一定的转化关系, 关于这种关系的研究也是十分重要的方向. 还有一类移位寄存器, 称为带进位的反馈移位寄存器(FCSR), 虽然 eSTREAM 计划中基于 FCSR 设计的算法最终被发现不安全, 但不能排除基于 FCSR 构造新的流密码算法的可能性, 这一类移位寄存器始终也是一种可选择的潜在序列源.

2.1.2 布尔函数

布尔函数在流密码中也是常见的一个基本模块, 一个具有 n 个变量的布尔函数 $f(x_1,x_2,\cdots,x_n)$ 可以看成如下的一个映射 $f:F_2^n\to F_2$. 它有多种表示形式, 即真值表表示、小项表示、多项式表示和 Walsh 谱表示, 常用的多项式表示是将一个布尔函数表示成变元的升幂及下标字典序写出的多个单项式之和, 这种表达形式称为代数正规型(ANF). 每个布尔函数的 ANF 是唯一的, 且其中非零系数的乘积项之最高次数记为这个布尔函数的代数次数. 布尔函数的选择对于流密码的安全性质有很大的影响, 其各种性质, 比如平衡性、相关免疫性[24]、非线性度、代数免疫度、线性结构等都曾是过去一些时段的研究热点问题, 但目前都已不再是关心的焦点问题, 文献[24]是布尔函数研究方面一个重要的里程碑, 直接启发了后来代数免疫度等指标的提出. 布尔函数性质的研究需要与算法对于相关攻击、线性分析及代数攻击等具体攻击场景相结合才可以获得较为持久的生命力. 在设计流密码时, 特别是一些轻量级算法时, 可以按目前公认的准则选取一些各方面性质较为平衡的布尔函数作为算法模块.

2.1.3 S 盒

S 盒可以看作其输入变元的向量布尔函数, 其使用在分组密码中非常普遍, 近年来随着基于扩散与混淆模块在流密码中的广泛使用, S 盒在流密码设计中也变得常见起来. 一个 (n,m)-S 盒可以看成一个如下的非线性映射 $f:F_2^n\to F_2^m$, 这个映射可以表示成一个真值表或者分量函数的 ANF. 多数 S 盒是静态的, 即对于确定输入攻击者知道其确定输出; 但也存在依赖于密钥的 S 盒, 当攻击者不知道密钥取值时, 因此也就不知道 S 盒在当下的具体形式. 最常见的 S 盒是 AES 算法中使用的 (8,8)-S 盒, 这一 S 盒可以看作有限域 $\mathrm{GF}(2^8)$ 上的多项式, 在数个流密码算法中, 比如 SNOW 2.0 和 SNOW 3G 等, 都采用了这一设计. 对于 S 盒之各种性质的研究需要与具体攻击场景结合以发挥出效力, 否则很容易无的放矢.

2.1.4 随机洗牌(Random Shuffle)的表

为了追求软件实现的高效率, RC4 等一系列算法均使用了随机洗牌的表. RC4 是一个面向字节而设计的流密码, 其使用一个包含 0 至 255 个数值的表, 在其上定义一个置换以生成密钥流. 虽然关于 RC4 算法的初始化阶段和初始密钥流统计特性已有了大量的分析结果, 但到目前为止, 在抛弃掉足够长度的初始密钥流字节后, 其密钥流生成阶段仍然被认为是十分安全的, 特别是对于 128 比特安全性而言. RC4 算法激发了随后大量的基于表而设计的流密码算法, 这些算法普遍具有较快的软件实现速度, 其状态恢复攻击往往需要极高的时间复杂度, 在软件实现的场合是一类非常合适的选择. 目前对于这类流密码的认识还处在发展的阶段, 如何有效地恢复这类算法的内部状态是一个十分重要的研究问题. 由于 RC4 在实际中得到了大量的应用, 对于 RC4 算法本身及其各类变体的研究具有十分重要的意义, 甚至有观点认为 RC4 算法就是流密码的核心算法之一, 在 RC4 本身获得的任何有影响力的分析结果都有可能带来对于这类构造流密码方式的认识飞跃. 目前在这类算法中, 还有 eSTREAM 计划的胜选算法之一 HC-128, 其采用两个表互控的方式来更新内部状态, 本质上是交错生成器思想与 RC4 算法设计理念的一种结合, 其软件实现速度很快, 但目前还缺乏有效的分析方法与手段, 这也从另一方面限制了这类算法在实际中的进一步应用.

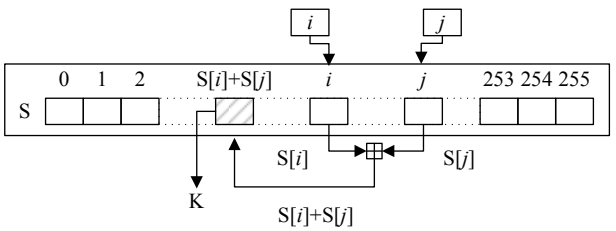

图 2 RC4 的密钥流生成

Figure 2 The keystream generation of RC4

2.2 流密码设计的发展及现状

公开文献中的流密码设计经过了较为长时间的发展历程, 下面我们对常见的一些流密码设计方法进行分类和总结.

2.2.1 基于 LFSR 的流密码

如前所述, Rueppel[1]将流密码的设计分成两个部分: 驱动部分和非线性组合部分. 驱动部分用于生成具有良好特性的基础源序列, 比如可以采用 *m*-序列等, 而非线性组合部分主要用来破坏密钥流序列的各种线性性质, 生成加密用的密钥流.

最常见的一种结构就是采用一个或者多个 LFSR 作为驱动部件来生成密钥流序列, 这主要是因为 *m*-序列具有非常大的周期以及良好的统计性质, 同时这类流密码已有成熟的理论分析结果, 并且在软件和硬件上实现起来都能达到很高的效率. 通常有三种方法来实现源序列的非线性化.

第一种是非线性组合生成器, 这种结构通常使用多个 LFSR 和一个非线性组合部件构成, 如图 3 所示.

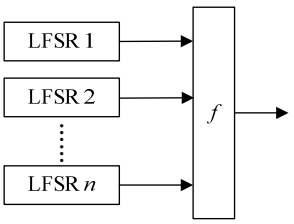

图 3 非线性组合生成器

Figure 3 Non-linear combination generator

密钥流的生成是通过一个非线性布尔函数 f 作用于多个LFSR的输出, 这个函数 f 被称为非线性组合函数. 如果 n 个 LFSR 的长度分别为 $l_1,l_2,\cdots,l_n$, 那么密钥流序列的线性复杂度变为 $f(l_1,l_2,\cdots,l_n)$, 由此可见这种设计方法使得线性复杂度大大增加. 组合函数的选取需要在非线性度, 相关免疫阶及代数次数与代数免疫度之间达到一个较好的平衡.

在 1985 年美密会上, Rueppel[1]首先提出了带记忆的非线性组合生成器, 他推广了无记忆组合函数相关免疫的概念, 并在此概念下证明了带记忆的非线性组合生成器可同时达到高的相关免疫阶和高的非线性度. Rueppel 认为具有 n 个输入的带记忆组合生成器可能达到相关免疫阶的最大值 $n-1$. 在 1992 年, Meier 和 Staffelbach[10]考察了带 1 比特记忆组合生成器, 并发现当前的输出与从初始时刻到当前时刻所有输入序列的线性函数的相关系数平方和是一个常数, 并指出带 1 比特记忆的组合生成器也具有类似无记忆组合生成器的"能量守恒定理". 随后在 1996 年, Jovan Dj.Golic[25]把之前的理论结果推广到了带多比特记忆的组合生成器中, 证明了带 r 比特记忆的组合生成器, 连续 $r+1$ 个输出与对应的连续 $r+1$ 组输入之间必然存在相关性. 带记忆单元的非线性组合生成器因其具有良好的密码学性质而广受重视, 在理论和实践上都有着广泛的应用. 在理论分析结果的基础之上, 1999 年"蓝牙特别兴趣组"公布了一个基于带记忆组合生成器而设计的蓝牙加密算法 E0[26], 它用来在无线及蓝牙网络中进行点对点通信的加密, 保证蓝牙通信安全性. E0 的结构是一个典型的带有 4 比特记忆的非线性组合生成器. 由于实际中蓝牙设备及 WIFI 的普及, 对于 E0 的分析受到国内外许多学者的重视, E0 的具体结构如图 4 所示.

由图 4 可知, E0 算法是加法生成器的一种改进, 在实际应用中, 由于二级结构的存在及每帧数据只有 2790 比特长, 这大大限制了各种攻击的直接使用, 需要结合具体环境来构造攻击.

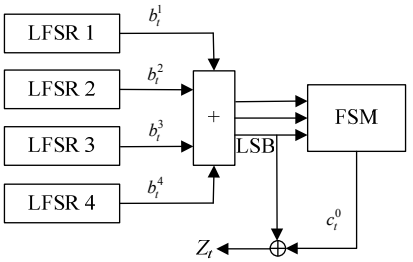

图 4　E0 算法核心部件
Figure 4　The E0 core

第二种是非线滤波生成器, 这种结构只使用一个LFSR, 密钥流是通过一个非线性函数 f 作用于LFSR的某些内部状态直接产生的, 如图 5 所示.

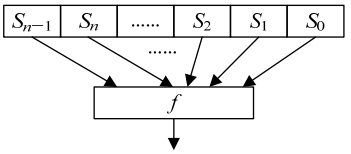

图 5　非线性滤波生成器
Figure 5　Non-linear filter generator

其中函数 f 函数被称为滤波函数. 如果 LFSR 的长度是 n 并且 f 具有非线性度 m, 则密钥流的线性复杂度最多为 $L_m = \sum_{i=1}^{m} \binom{n}{i}$. 采用这类结构设计的流密码算法非常多, 并且应用也非常广泛, 比如 ISO/IEC 国际标准加密算法 SNOW 2.0[27], 以及 3GPP LTE 国际加密标准算法 SNOW 3G 和 ZUC[28]等. 下面我们给出 SNOW 2.0 的结构图, 见图 6.

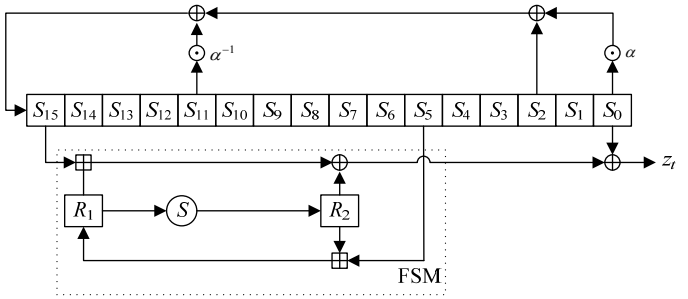

图 6　SNOW 2.0 算法结构
Figure 6　The schematic of SNOW 2.0

从图 6 可以看出, SNOW 2.0 在非线部分采用了带有 2 个记忆单元的有限状态自动机(FSM), S 变换用到了 AES 的 S 盒和 Mixcolumn. 由于 SNOW 2.0 所用的线性反馈移位寄存器定义在扩域上, 这种设计非常便于软件实现. 这种结构的设计采用了 Rueppel 的线性驱动加非线性混淆的思路, 但非线性部分采用了类

似分组密码扩散与混淆的结构, 具有很高的安全性. 在 eSTREAM 计划最终胜选的算法中, 也存在类似结构的算法, 比如 SOSEMANUK[3]算法采用了和 SNOW 2.0 基本相同的结构, 并且在非线性部件中使用了 Serpent 的 S 盒作为基本元件.

第三类是钟控生成器, 这类流密码设计至少使用一个LFSR, 这个LFSR按某种规则进行不规则钟控输出. 在交错生成器(Alternating Step generator)中, 一个 LFSR 的输出决定另外两个 LFSR 哪一个应该运行. 在自收缩与收缩生成器(Self-shrinking generator[29], Shrinking generator[30])中, 按缩减原则进行输出, 比如在收缩生成器中, 两个 LFSR 正常运行, 如果第一个 LFSR 的输出是 1, 那么第二个的对应输出作为密钥流的输出, 否则不输出. 钟控生成器的设计要避免不规则钟控带来的输出效率的降低, 在这方面, A5/1 的设计是一个很好的范例. 钟控类流密码中最著名且应用最广泛的就是用于 GSM 加密的 A5/1 算法, 其算法结构如下图所示.

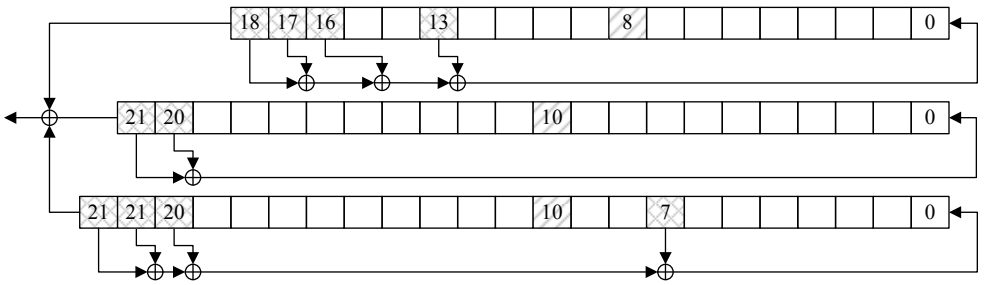

图 7 A5/1 算法结构
Figure 7 The schematic of A5/1

A5/1 算法的钟控结构较好的解决了输出效率问题, 目前的分析主要是相关攻击, 时间存储数据折衷攻击和猜测确定攻击. 对于 A5/1 的分析表明流密码的内部状态大小对于算法安全性有较大的影响, 需要选择至少两倍于密钥长度的内部状态来获得希望的安全性. 例外一个比较著名的钟控流密码算法是 LILI-128, 但是这个算法同样也存在一些安全性问题, 之后采用钟控设计的流密码算法非常少, 最近的基于钟控的流密码算法是 eSTREAM 计划中面向硬件的胜选算法 MICKEY 2.0. 但是 MICKEY 2.0 虽然采用了钟控结构, 但是它和以前的钟控流密码算法结构截然不同, 它采用的是两个寄存器之间相互控制, 相互影响的方式, 具体如下图所示.

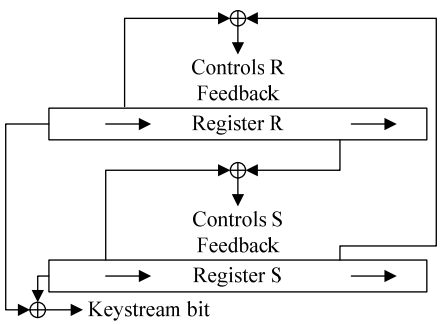

图 8 MICKEY 2.0 算法结构
Figure 8 The schematic of MICKEY 2.0

2.2.2 基于分组密码工作模式和结构的流密码

利用分组密码的工作模式, 可以将分组密码转换为流密码. 在假设所使用分组密码是安全的时候, 这些工作模式可以提供某些可证安全性.

密文反馈模式(CFB)将分组密码变换为一个自同步的流密码, 其结构如图 9 所示. 密文反馈模式主要优点是具有有限的错误传播, 可以用于认证, 也可实现自同步功能. 缺点是加密效率比较低, 加解密两端都需要用到分组密码的加密器.

输出反馈模式(OFB)和 CFB 模式的结构非常类似, 但是所得到的流密码是同步流密码而不是自同步的流密码. 不是加密上一个分组的密文而是对上一个分组的密钥流进行加密. 具体结构如图 10 所示.

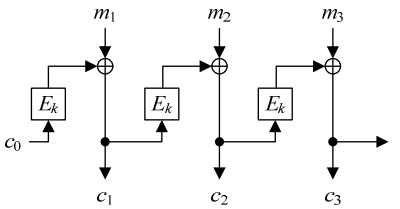

图 9 密文反馈模式
Figure 9 The cipher feedback mode

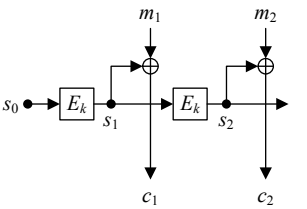

图 10 输出反馈模式
Figure 10 The output feedback mode

计数器模式(CTR)比其他模式更新, 密钥流的生成通过加密一个有 IV 和计数器组成的分组. 计数器可以是任意函数 $f(i)$, 最简单并且最广泛的选择是令 $f(i)$ 是一个真实的计数器, 即 $f(i)=i$. 这种工作模式的优点就是安全高效, 可并行, 并且适合任意长度的明文信息. 在加解密过程中只用到了加密算法, 因此在实现时无需实现解密算法.

基于分组密码设计的算法不仅仅局限于工作模式, 还有很多采用分组思想而设计的流密码. 在 eSTREAM 计划胜选算法中, Salsa 20 生成密钥流的过程和分组密码非常类似, 每次都是对 16 个字的初始状态进行轮函数迭代变换, 将最终变化后的状态作为密钥流输出. 图 11 展示了 Salsa 20 算法的轮函数的一个小轮, 整个轮变换是需要进行多个这样的小轮, 这和分组密码的工作过程类似.

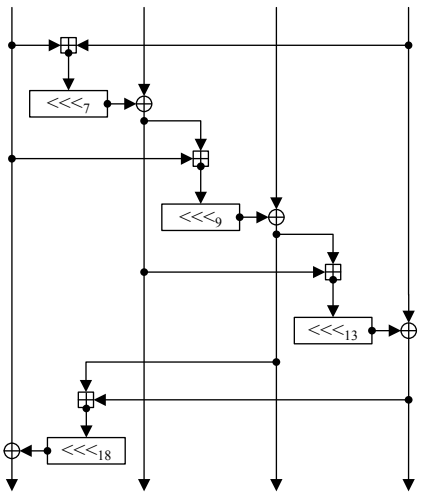

图 11 Salsa 子轮函数
Figure 11 The Salsa quarter-round function

这是分组密码设计思想在流密码中的一种应用形式, 还有另外一种设计思路, 就是采用和分组密码基本相同的运行流程, 但是每次从轮变换之后的输出中抽取某些中间状态, 并通过简单的运算作为密钥流输出. 这种结构的典型流密码算法是 AEGIS[31], 这个算法是 CAESAR 竞赛中提交的算法, 它的轮函数如图 12 所示.

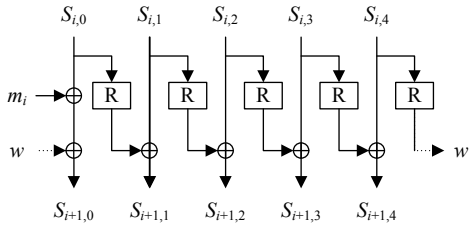

图 12 AEGIS 轮函数
Figure 12 The AEGIS round function

这类算法的优点就是其软件实现非常快, 并且从流密码角度来看, 由于其内部状态非常大, 并且不存在移位寄存器结构, 在分析过程中传统的流密码分析方法很难应用.

2.2.3 基于非线性反馈移位寄存器的流密码

自 eSTREAM 计划和 CAESAR 竞赛之后, 流密码的设计不再局限于传统的设计方法, 许多新的设计思路和设计方法层出不穷, 大大丰富了流密码的设计方法. 下面我们介绍一下其中比较典型的流密码算法.

这类算法中以 NFSR 作为基本组件之一, 采用非线性反馈与非线性输出相结合的办法提供非线性性质与安全性. eSTREAM 计划中的 Grain v1 算法就是将 LFSR 和 NFSR 相互结合. 其结构如图 13 所示.

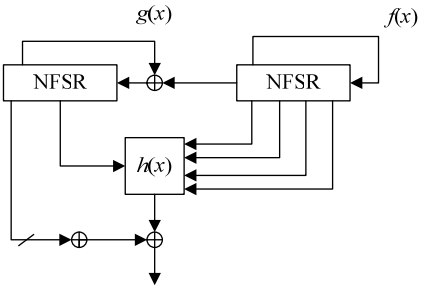

图 13 Grain v1 算法结构
Figure 13 The schematic of Grain v1

Grain v1 算法的特点是利用 LFSR 提供良好统计特性的同时又加入了 NFSR 的非线性扰动. 由于 NFSR 的研究还处在起步阶段, 目前现有的方法对基于 NFSR 而设计的算法都不太有效, 想要恢复 NFSR 的内部状态还是非常困难的. 同样, eSTREAM 计划最终入选算法中的 Trivium 也是基于 NFSR 结构, 它用了三个 NFSR 相互串联来构成内部状态, 并经过简单异或操作来产生密钥流, 其结构见图 14. 对于目前这些基于非线性反馈移位寄存器而设计的流密码, 传统的周期与线性复杂度分析都很难从理论上进行说明, 只能依赖计算机实验来验证这些性质; 但另一方面, 由于这些算法的内部状态往往很大, 因此从理论上讲, 其存在较小状态转移圈的概率很小, 在实际中可以忽略不计. 最为重要的是, 基于非线性反馈移位寄存器的流密码算法的安全性分析, 目前还没有统一的模式和路线, 但可以预计的是, 这些算法在未来相当长时间内都将是很主流的一类设计方案, 对其进行密码分析具有十分重要的意义.

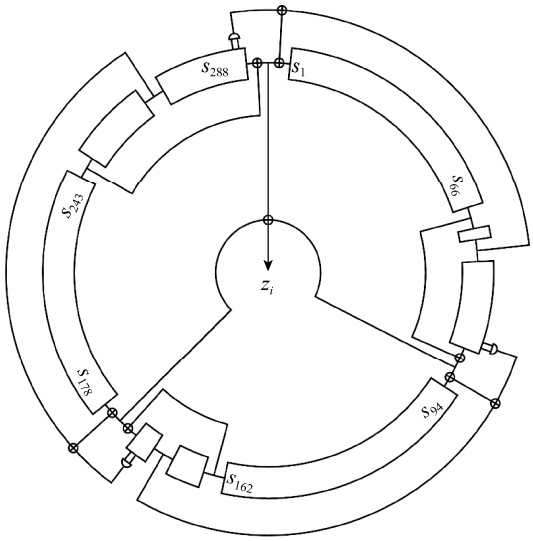

图 14 Trivium 算法结构
Figure 14 The schematic of Trivium

2.2.4 基于置换/Sponge 结构的流密码

由于 Keccak 在 SHA-3 竞赛中的胜出, 最近出现了一种基于置换/Sponge 结构的流密码——ICEPOLE, 其基本思想就是利用 Keccak 的部分内部状态直接输出作为密钥流序列, 结构如图 15.

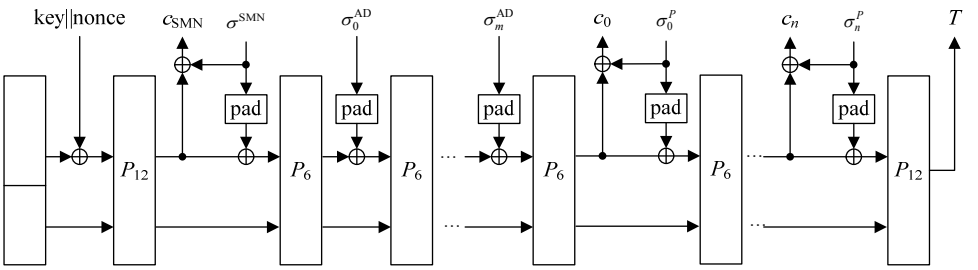

图 15 ICEPOLE 算法结构
Figure 15 The schematic of ICEPOLE

这种结构的流密码其优点在于它能够很自然的提供认证功能, 而不需要额外的认证模块, 只要哈希函数的轮函数具有很好的安全性质, 就能够提供较高的安全性. 可以预期, 这类结构的流密码在未来会得到大大发展, 利用这种结构, 新的更好的流密码算法将会出现. 但其安全性分析也是一个亟待解决的问题, 这也是未来十分有意义的研究方向. 从实现的角度看, 其中采用的置换究竟需要多少的轮数, 也是一个十分重要的问题. 从密码分析的角度来看, 这类算法是否存在目前还未知的弱点也是一个十分重要的问题.

最近在 Eurocrypt 2016[32]上, 为了满足全同态加密的要求, 最小化时间和存储的实现以及提高同态容量, 一种新的流密码结构被提出, 它们将这种结构称为置换滤波生成器(filter permutator). 这种结构的流密码只用到了置换和一个非线性过滤函数, 基于此新提出了一个流密码 FILP, 其结构如图 16.

这个算法的特点就是密钥长度远远大于安全界, 其最新版本采用 530 比特的密钥长度, 但是所达到的安全界却很低, 仅为 80 比特. 从目前仅有的分析结果来看, 这种结构对滤波函数的选择要求非常高, 否则

会很容易进行分析, 泄露出大量的密钥信息.

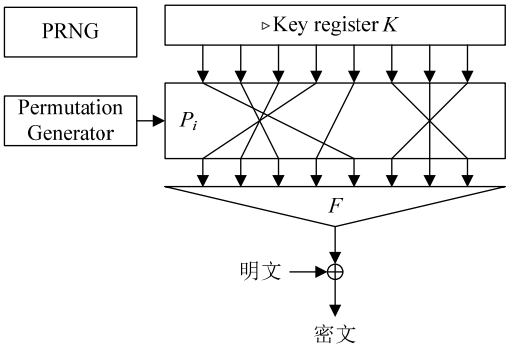

图 16 FLIP 算法结构
Figure 16 The schematic of FLIP

综上所述, 我们介绍了流密码发展至今出现的众多的著名设计方法, 并给出了这些设计方法中一些典型的流密码实例; 针对这些不同的设计方法, 我们分析了其设计的一些优点, 希望能对以后设计新的流密码算法起到一些启发作用.

2.3 流密码分析的发展及现状

众所周知, 流密码的攻击可分为密钥/明文恢复攻击和区分攻击两大类, 任意一个密钥/明文恢复攻击同样也是一个区分攻击, 通常意义下的区分攻击相对弱于密钥恢复攻击. 曾经有学者争辩过一个流密码存在复杂度比安全界低的区分攻击是否意味着该算法被攻破, 后来在 NESSIE 计划中, 达成的一致意见认为一个安全的密码系统不应该存在任何能够以低于安全界的复杂度可发现的缺陷. 在前面引言部分已经详细叙述了流密码的主要分析方法, 这里不再重复已讲过的内容, 而只是对于相关攻击和线性分析进行进一步阐述.

2.3.1 相关攻击

相关攻击从对基于 LFSR 流密码的分析起步, 最早由 Blaser 和 Heinzmann 提出, 但真正有价值的工作出现在 1985 年, Siegenthaler [8]提出了非线性组合生成器的分别征服相关攻击, 其思想是利用组合函数的输出和输入分量或某些输入分量子集之和的相关性, 穷搜某个特定 LFSR 的初始状态或者某几个 LFSR 的初始状态, 而各个 LFSR 的初始状态就是非线性组合流密码的子密钥. 这就是最早的相关攻击方法.

随后在 1998 年, W.Meier 和 O.Staffelbach[15]给出了加速上述分别征服相关攻击的两个算法(算法 A 和算法 B), 称为快速相关攻击, 其出发点是上述相关攻击的复杂度与 LFSR 的长度成指数关系, 因此这类攻击只能用于长度较短的 LFSR. 针对此问题, W.Meier 和 O.Staffelbach 对 LFSR 的抽头数较少的非线性组合流密码提出了一种使用概率迭代译码算法的快速相关攻击, 不需要搜索整个 LFSR 的所有可能初始状态就能找出正确的初始状态. 这个方法是相关攻击发展的里程碑, 之后对于相关攻击的研究进入了鼎盛阶段, 各类文章层出不穷.

上述经典工作之后, 又陆续出现了对于相关攻击核心思想的改进方法, 这是相关攻击发展的非常重要的一个方面. 下面简单介绍一下这方面的几篇重要论文. 在 Asiacrypt 1996 上, 基于 R.Anderson[33]对于采用满足某些密码学性质的滤波生成器的条件相关攻击思想, Sangjin Lee[16]等正式提出了条件相关攻击的框架, 其核心思想考察增量函数在特定输出情况下, 输入变量的相关性. 在 2003 年, 条件相关攻击又被扩展到两种类型的攻击: hybird correlation attack 和 concentration attack[17]. 这两种攻击的目标都是恢复 LFSR 未知的初始状态, 通过条件相关攻击和快速相关攻击. 在 2005 年 CRYPTO 上, Lu-Meier-Serge[18]等人把条

件相关攻击扩展为在猜测部分未知输入的情况下, 考察向量函数输出的相关性, 这里假定部分输入信息服从随机均匀分布; 特别的, 这个方法在攻击二级蓝牙加密算法 E0 时被证明非常有效. 这是相关攻击的一个重要发展, 且是在核心方法上进行了改进, 将传统的相关攻击有效地扩展为条件相关攻击.

通常情况下, 相关攻击都可以被看作是一个译码问题, 这里将 LFSR 的输出序列看作是发送的码字, LFSR 的初始状态看作信息位, 将非线性组合生成器或者带记忆有限状态机看作一个噪声信道, 通常用二元对称信道(BSC)对其进行刻画, 而密钥流序列则可以看作是通过信道发送传输后所收到的码字. 根据 Shannon 编码理论, 当收到的密钥流序列满足一定的条件时, 就能够进行成功译码.

快速相关攻击的研究多集中于译码方式和如何寻找低重量的校验等式. 在快速相关攻击中, 如何快速高效地寻找校验等式是非常重要的一个问题. 最早, Meier 等考虑的是 LFSR 的低重量反馈多项式 $g(x)$. 通过二元域上多项式的性质, 可以通过平方或者移位来获得新的校验等式. k 的取值是由 $g(x)$的次数以及所能获得的密钥流长度决定的. 如果 LFSR 不存在这样的低重量反馈多项式或者攻击者想要获得更多的校验等式, 这种方法是不可行的.

Mihaljevic 和 Golic[34]描述了怎么使用加密算法的 LFSR 的变换矩阵来产生校验等式. 假设 LFSR 的长度是 l 以及最大长度为 N, 那么使用他们的算法能够寻找到

$$m=\binom{l}{t+1}\frac{N}{l2^{t}}$$

个校验等式, 当 l 较大时, 该方法的复杂度偏高.

Chepyzhov 和 Smeets[35]使用编码的方法, 包括 Gilbert-Varshamov 界来寻找校验等式, 所需要的复杂度为 $O\left(2^{(1-l/N)l}\right)$, 这个方法只适用于 l 较小的情况或者相关系数很大的情况.

1999 年 Eurocrypt 上, Johansson[14]等人对快速相关攻击做了重要的改进, 他们基于卷积码理论提出了一种新的快速相关攻击方法. 与之前方法不同的是, 这个方法可以应用于任意形式的 LFSR 反馈多项式, 而之前一些方法主要适用于低重量的反馈多项式. 随后 2000 年 Eurocrypt 上, Anne Canteaut[11]等也提出了快速相关攻击的一种新技术, 这个方法是基于 Gallager 的对重量大于 3 的校验等式的迭代概率译码算法. 这些攻击同样能够应用于任意的基于 LFSR 的密钥流生成器, 并且不要求反馈多项式具有低重量. 他们分析了当时所有的快速相关攻击, 并且指出了这个算法在校验等式重量为 4 或 5 的时候比基于卷积码或 turbo 码的相关攻击更加有效. 同一年在 FSE 上, V. Chepyzhov[36]等也提出了一个新的快速相关攻击简便算法. 他们的攻击方法比起以前一些攻击方法在空间复杂度上有所降低, 这个算法能够非常的简洁得到一些理论结果, 可以很好的对数据量、相关概率、计算复杂度和成功概率做出可靠的理论估计, 特别适用于无法进行计算机模拟实验的情况. 在 2001 年, Golic[37]提出了将编码理论过中最优的逐符号译码算法 H-R 算法应用于快速相关攻击, 从而得到了一种新的基于迭代概率译码算法的相关攻击. 这个攻击方法可以应用于包含大量非正交的校验等式的情况. 在 2002 年 Eurocrypt 上, Philippe Chose 等提出了一些对快速相关攻击进行改进的算法, 在以前关于快速相关的论文中, 算法本身从来都不是关注的主题, 该论文集中讨论了寻找最佳算法来发现和估值校验等式. 这篇文章指出, 使用简单算法来寻找和估值校验等式应该被具有更好的渐进复杂度的算法所替代, 使用更加高级的算法技术来加速整个过程. 这种新算法可以对快速相关攻击的效率带来很大的提高. 由最初的快速相关攻击知, 如果反馈多项式的重量较低, 快速相关攻击将非常有效. 在 FSE 2004 上 Hakan Englund[38]等发现了一类新的弱反馈多项式. 这类多项式可以具有很高的重量, 但能够十分有效地实施相关攻击.

近些年来关于快速相关攻击的文章比较少, 原有相关攻击的一些技术都趋于成熟. 最新的研究成果多集中在对以前相关攻击中存在的一些缺点的改进. 比如在 SAC 2006, 我们[39]指出以前的结果主要是把 LFSR 的初始状态看成一个整体, 并且仅仅使用一种校验等式来进行译码; 但实际上可以充分利用不同种类的校验等式, 在不增加渐近复杂度的情况下, 逐部分地恢复初始状态, 并且对反馈多项式的重量没有要

求和限制. 在 FSE 2007 上, Carlet[40]等通过对向量布尔函数的分析, 提出了广义相关攻击的概念. 它是基于输入的线性逼近表达式, 但是输出的次数没有限制. 通过实验结果他们发现新的广义相关攻击给出的线性逼近具有更大的偏差.

2.3.2 线性分析

区分攻击的目的是试图区分截获的密钥流和完全随机的序列, 区分攻击通常比密钥恢复攻击要弱, 但是区分攻击依然能够说明密码算法所存在的某些缺陷. 线性分析在流密码区分攻击中有着广泛的应用.

线性分析是一种通用的密码分析方法, 其试图寻找密码系统的有效仿射逼近: 在 1993 年的 Eurocrypt 上, 日本学者 Matsui [5]提出了的关于 DES 分组密码的线性分析, 其主要思想是通过对 DES 进行逐步地仿射逼近来寻找一个关于算法总体的线性区分器. 这里的有效区分器是指包含输入明文、输出密文和密钥信息的逼近等式以不同于 1/2 的较显著概率成立. 在 1994 年 CRYPTO 上, B. Kaliski 等提出了一个线性分析的新技术—多线性分析, 这种技术可以非常有效地降低数据复杂度, 但是由于限制条件比较多, 还仅限于应用到 DES.

线性分析早在 1989 年和 1990 年就应用于流密码分析中, 后来在 1996 年, Golic[9]指出任意的带 M 比特记忆的二元密钥流生成器可以被线性化为一个长度至多为 M 的非自治线性反馈移位寄存器和附加输入为非平衡的二元随机变量序列, 文章提出了一个确定线性模型的方法, 它是基于自制有限状态机的 linear sequence circuit approximation 方法(LSCA), 并通过这种方法得到了钟控移位寄存器和任意的移位寄存器的线性模型. 在 Golic 的经典工作之后, 关于线性区分攻击在流密码中的应用比较少见, 直到 2002 年的 CRYPTO 上, Don Coppersmith[6]等描述了一种新的密码分析技术 linear masking, 它可以用来区分流密码和真实的随机过程. Linear masking 方法主要应用于由线性过程和非线性过程组成的流密码, 寻找线性部分的一些线性组合, 把线性部分消去, 只保留非线性部分. 因此在攻击时只需要关注非线性部分, 在非线性部分寻找用来区分的特征. 作者把 linear masking 用于分析 SNOW 1.0 并得到了比较好的理论结果. 之后线性攻击的发展多集中于多维线性分析方面, 相比较于以前的线性分析, 多维线性分析是一个更为有效的线性分析方法, 它能够更为有效地利用较多的线性逼近关系. 随后在 2004 年 CRYPTO 上, Alex Biryukov[41]等研究了多线性分析, 提出了多线性分析的理论统计框架, 同时他们将 Matsui 的算法 1 和算法 2 推广到多线性的情况.

目前线性分析的热点多集中在怎样利用多个线性逼近来进行线性分析, Miia Hermelin[42]等在 ACISP 2008 上提出了对 Matsui 算法 1 的一个新的真正的多维方式的扩展. 在理论上建立了一个统计框架, 通过一维线性逼近来计算多维概率分布. 这个框架的主要优点就是可以取消线性逼近之间的独立性, 文章中利用多维线性分析对 Serpent 进行了分析, 结果表明在一定的缩减轮数下比一维的线性逼近更加有效.

通过线性分析的发展过程可以看出, 在线性分析中如何寻找比较好的线性逼近是是非常重要的一个步骤, 如何能够充分利用找到的一些线性逼近来构造高效的多维区分器也是非常重要的. 另外一个研究方向是对区分器本身的研究, 如何构造区分器, 利用一些统计理论对区分器的性能进行估计等.

3 流密码设计与分析中一些新的研究成果

下面我们简要叙述一下我们关于流密码分析的一些较新的研究成果, 希望对以后相关的研究起到抛砖引玉的作用.

3.1 FSE 2013上Grain v1流密码的分析

我们在 FSE 2013 上[43]给出了流密码算法 Grain v1 的 near-collision 攻击, 文章提出了一种 near-collision 的概念(见定义 2), 发现了 Grainv1 算法的如下特点, 在密钥流生成阶段, LFSR 的更新过程是完全独立的, 不受任何其他组件的影响. 如果 LFSR 和 NFSR 两个 160 比特内部状态在两个不同时刻, 他们大多数的比特都相同, 只有极少数的位置不同, 那么它们产生的密钥流前缀也将非常相似, 两个密钥流之间的差分并

不能取遍所有的值, 因此输出的密钥流差分的分布是非常不均匀的. 某些差分出现的概率非常高, 而有些差分却非常低. 利用这个特点, 在两段密钥流截断满足以上性质时, 就可以利用密钥流差分分布来导出内部状态的差分, 而一旦知道了内部状态的差分, 那么就很容易可以恢复 LFSR 的内部状态, 再结合其他技术就能够恢复出 NFSR 的内部状态.

定义 2(near-collision) 给定两个子集 A 和 B, 其中每个元素都属于 $\mathrm{GF}(2)^n$, 那么存在一个对 $(a,b)\in(A,B)$ 是 d-near-collision, 其中 $a\in A$ 和 $b\in B$, 如果这两个集合满足

$$|A|\cdot|B|\geqslant\frac{2^n}{V(n,d)}$$

其中 $|A|$ 和 $|B|$ 是 A 和 B 的大小.

目前关于该攻击的工作仍然在继续进行中.

3.2 CRYPTO 2013上条件相关的进一步扩展和E0算法的分析

我们在 CRYPTO 2013 上[19]中对 CRYPTO 2005 上[18]中提出的条件相关攻击进行了推广, 通过引入条件掩码的概念(见定义 3), 提出了一种基于条件掩码的条件相关攻击, 这种分析方法称为 condition masking. 我们在 condition masking 下研究了 E0 算法的条件相关特性, 将 E0 算法攻击的目标函数的条件相关推广到同时依赖于线性掩码和条件掩码. 基于 condition masking 方法, 我们构造了 E0 的条件相关线性逼近. 通过这个新的条件相关并结合向量方法, 给出了更好的关于 E0 算法的分析结果.

定义 3 给定函数 $h:\mathrm{GF}(2)^u\times\mathrm{GF}(2)^v\to\mathrm{GF}(2)^r$, 其输入为 $B\in\mathrm{GF}(2)^u$ 和 $X\in\mathrm{GF}(2)^v$. 其中二元向量 B 包含密钥的相关信息, 它在条件相关攻击中被称为条件向量. 令 $B=(b_0,b_1,\cdots,b_{u-1})\in\mathrm{GF}(2)^u$ 和 $\lambda=(\lambda_0,\lambda_1,\cdots,\lambda_{u-1})\in\mathrm{GF}(2)^u$, 其支撑集

$$\mathrm{supp}(\lambda)=\{0\leqslant i\leqslant u-1\,|\,\lambda_i=1\}=\{l_1,\cdots,l_m\}\,(l_j<l_{j+1})$$

那么对于向量 B, 其由 λ 定义的截断向量 $B'=(b_{l_1},\cdots,b_{l_m})\in\mathrm{GF}(2)^m$. 这里我们把 λ 称为 B 的条件掩码. 另外, B 中的剩余比特组成一个新的向量, 并且把它定义为 $B^*\in\mathrm{GF}(2)^{u-m}$, 它包含 B' 的互补比特. 我们定义一个操作'\'用来表示上面的过程, 这样我们有 $B^*=B\setminus B'$.

3.3 CRYPTO 2015上扩域上的快速相关攻击和SNOW 2.0的分析

我们在 CRYPTO 2015 上[44]对传统的相关攻击进行了扩展, 将传统的相关攻击推广到了扩域上面, 提出了扩域上快速相关攻击的完整算法, 并解决了相关攻击提出者给出的公开问题. 我们构造了扩域上快速相关攻击的一般框架, 并且给出了这个框架的所有理论分析, 包括预计算阶段复杂度的理论估计以及在线阶段译码复杂度的估计. 在预计算阶段, 应用 Wagner 的 k-tree 算法来生成需要的目标校验等式, 而在线阶段, 我们提出了两个快速的译码算法. 译码模型采用了一般的离散无记忆信道(DMC), 并且首次在理论上建立了 DMC 的信道容量和噪声的 SEI 的关系式. 同时还给出了对于原始的大单位的线性逼近可以映射到许多低维数的空间上, 从而来降低数据以及预计算的复杂度; 在在线阶段, 可以采用快速 Walsh 来获得更好的译码复杂度. 我们最后将上面的方法应用到 SNOW 2.0 上, 如前所述, 这是一个 ISO/IEC 18033-4 国际标准算法, 并且还曾作为欧洲 eSTREAM 计划中的基准算法, 我们给出了 SNOW 2.0 其非线性部份 FSM 的字节级线性逼近. 通过 $\mathrm{GF}(2^8)$ 上的快速相关攻击来恢复出 LFSR 的初始状态. 攻击的时间、存储、数据以及预计算的复杂度都是低于 $2^{186.95}$; 我们进一步改进了攻击结果, 通过把原来简单的 $\mathrm{GF}(2)$ 上的线性掩码变为 $\mathrm{GF}(2^8)$ 上的有限域线性掩码, 使得攻击的时间、存储、数据以及预计算之复杂度都低于 $2^{164.15}$.

4 发展趋势与展望

对于流密码的研究已经过去了几十年, 无数的学者为流密码的研究做出了许多重要的贡献. 相应地, 流密码的设计, 也从一次一密到基于 LFSR 的流密码, 再到现在的基于非线性反馈移位寄存器的算法和各种多样化的设计.

一些最新的算法利用了分组密码的轮函数作为组件来设计流密码. 传统的基于 LFSR 的设计方法, 在新的设计思路面前已经被摒弃了, 从而使得现在流密码的分析越来越困难, 但有理由相信, 面向新设计的崭新分析方法终将崭露头角. 在硬件和软件的速度方面, 尽管分组密码的实现效率已经相当可观, 但流密码的固有优势并不会日趋减小; 相反, 流密码在新的编程指令下会表现出更明显的速度优势. 因此, 在未来的密码学发展中, 流密码的地位依然重要, 并且可能逐渐加重比率. 这一方面是因为流密码成熟的理论和广泛的应用, 使得流密码日益深入到我们的现实生活中; 另一方面, 在某些特定的应用环境中, 也会不得不转而使用流密码以满足各种需求, 例如全同态加密方案中也会用到流密码作为其安全组件. 尽管目前流密码的研究不是密码学中的热点, 但随着密码学的发展, 流密码的地位可能会日益提升, 也必将会再有一次大的发展. 例如, 作为流密码中一个古老的分支, 带记忆流密码的分析已经变得越来越困难, 目前广泛应用的带记忆流密码, 大多都具有较高的安全性. 因此对其进行研究的价值也会越来越大, 一旦在理论上破解了某个带记忆单元的流密码方案, 一定会引起很大的轰动.

我们认为, 在未来的流密码研究中, 只有直接与流密码设计与分析相关的结果才会具有重要的理论和实际价值. 因此, 对于目前未来得及分析的一些算法进行深入研究是非常重要的方向. eSTREAM 计划中, 胜选算法 Sosemanuk[45]也是一个带记忆单元的流密码, 对它的分析是值得继续下去的. 在 3GPP 中的标准加密算法之一, SNOW 3G 也是一个可以继续做下去的目标. 这里, 相关攻击和线性分析依旧是可以采用的主要技术手段. 在未来的工作中, 快速相关攻击需要更深入的进行研究, 尤其是扩域上的快速相关攻击, 其复杂度以及其各种离线和在线阶段的算法还需要进一步的改进, 以使得相关攻击的理论更加完善. SNOW 2.0 的分析中, 如何能够使得复杂度进一步降低, 如何寻找一个新的攻击方法使得攻击复杂度低于 2^{128}, 是一个十分重要的研究课题, 并可以考虑线性一致性测试分析[46]. 在 E0 算法的分析中, 如何更进一步降低数据复杂度也是非常重要的. 由于蓝牙的传输速率是比较低的, 所以目前攻击的瓶颈是截获蓝牙数据所需要的时间太长, 一般蓝牙发生的数据帧都比较小, 而且时间也短, 因此如何有效降低数据量, 将会使得攻击更加符合蓝牙加密的实际情况.

综上所述, 未来对流密码的研究还是有很多方向值得继续做下去, 主要就是寻找新的设计思路, 寻求新的攻击方法, 以不断地加深对流密码本身的认识和理解.

References

[1] RUEPPEL R A. Analysis and Design of Stream Ciphers[M]. Springer-Verlag, 1986.

[2] DAWSON E, CLARK A, GOLIC J, et al. The LILI-128 keystream generator[C]. In: Proceedings of first NESSIE Workshop. 2000.

[3] HELL M, JOHANSSON T, MEIER W. Grain: a stream cipher for constrained environments[J]. International Journal of Wireless and Mobile Computing, 2007, 2(1): 86–93.

[4] Canniere C D, Preneel B. Trivium specifications[OL]. https://www.cosic.esat.kuleuven.be/ecrypt/stream/e2-trivium.html.

[5] MATSUI M. Linear cryptanalysis method for DES cipher[C]. In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer Berlin Heidelberg, 1993: 386–397.

[6] COPPERSMITH D, HALEVI S, JUTLA C. Cryptanalysis of stream ciphers with linear masking[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2002: 515–532.

[7] XIAO G Z, MASSEY J L. A spectral characterization of correlation-immune combining functions[J]. IEEE Transactions on Information Theory, 1988, 34(3): 569–571.

[8] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, 100(1): 81–85.

[9] GOLIĆ J D. Correlation properties of a general binary combiner with memory[J]. Journal of Cryptology, 1996, 9(2): 111–126.

[10] MEIER W, STAFFELBACH O. Correlation properties of combiners with memory in stream ciphers[J]. Journal of Cryptology, 1992, 5(1): 67–86.
[11] CANTEAUT A, TRABBIA M. Improved fast correlation attacks using parity-check equations of weight 4 and 5[C]. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2000: 573–588.
[12] CHOSE P, JOUX A, MITTON M. Fast correlation attacks: An algorithmic point of view[C]. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2002: 209–221.
[13] JOHANSSON T, JÖNSSON F. Fast correlation attacks through reconstruction of linear polynomials[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2000: 300–315.
[14] JOHANSSON T, JÖNSSON F. Improved fast correlation attacks on stream ciphers via convolutional codes[C]. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1999: 347–362.
[15] MEIER W, STAFFELBACH O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159–176.
[16] LEE S, CHEE S, PARK S, et al. Conditional correlation attack on nonlinear filter generators[C]. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 1996: 360–367.
[17] LÖHLEIN B. Attacks based on Conditional Correlations against the Nonlinear Filter Generator[J]. IACR Cryptology ePrint Archive, 2003, 2003: 20.
[18] LU Y, MEIER W, VAUDENAY S. The conditional correlation attack: A practical attack on Bluetooth encryption[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2005: 97–117.
[19] ZHANG B, XU C, FENG D. Real time cryptanalysis of Bluetooth encryption with condition masking[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 165–182.
[20] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003: 644–644.
[21] COURTOIS N. Fast algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003: 176–194.
[22] DINUR I, SHAMIR A, Cube attacks on tweakable black box polynomials[C]. In: Advances in Cryptology—EUROCRYPT 2009, Springer Berlin Heidelberg, 2009: 278–299.
[23] BABBAGE S H. Improved “exhaustive search” attacks on stream ciphers[C]. In: European Convention on Security and Detection, 1995. Springer Berlin Heidelberg, 1995: 161–166.
[24] SIEGENTHALER T. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.)[J]. IEEE Transactions on Information theory, 1984, 30(5): 776–780.
[25] GOLIC J D. Linear models for keystream generators[J]. IEEE Transactions on Computers, 1996, 45(1): 41–49.
[26] Bluetooth S: Specification of Bluetooth System-Version 4.0[S/OL]. http://www.Bluetooth.com.
[27] 3GPP. Specification of the 3GPP confidentiality and integrity algorithms UEA2& UIA2. Document 2: ZUC Specifications. Version: 1.1. ETSI[S]. 2010.
[28] EKDAHL P, JOHANSSON T. A new version of the stream cipher SNOW[C]. In: International Workshop on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2002: 47–61.
[29] MEIER W, STAFFELBACH O. The self-shrinking generator[C]. In: Advances in Cryptology—EUROCRYPT 1994. Springer Berlin Heidelberg, 1995: 205–214.
[30] COPPERSMITH D, KRAWCZYK H, MANSOUR Y. The shrinking generator[C]. In: Advances in Cryptology—CRYPTO 1993, Springer Berlin Heidelberg, 1993: 22–39.
[31] WU H, PRENEEL B. AEGIS: A fast authenticated encryption algorithm[C]. In: International Conference on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2013: 185–201.
[32] MÉAUX P, JOURNAULT A, STANDAERT F X, et al. Towards stream ciphers for efficient fhe with low-noise ciphertexts[C]. In: Advances in Cryptology—EUROCRYPT 2016. Springer Berlin Heidelberg, 2016: 311–343.
[33] ANDERSON R. Searching for the optimum correlation attack[C]. In: International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1994: 137–143.
[34] MIHALJEVIC M J, GOLIC J D. A method for convergence analysis of iterative probabilistic decoding[J]. IEEE Transactions on Information Theory, 2000, 46(6): 2206–2211.
[35] CHEPYZHOV V, SMEETS B. On a fast correlation attack on certain stream ciphers[C]. In: Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1991: 176–185.
[36] CHEPYZHOV V V, JOHANSSON T, SMEETS B. A simple algorithm for fast correlation attacks on stream ciphers[C]. In: International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2000: 181–195.
[37] GOLIC J D. Iterative optimum symbol-by-symbol decoding and fast correlation attacks[J]. IEEE Transactions on Information Theory, 2001, 47(7): 3040–3049.

[38] ENGLUND H, HELL M, JOHANSSON T. Correlation attacks using a new class of weak feedback polynomials[C]. In: International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2004: 127–142.
[39] ZHANG B, FENG D. Multi-pass fast correlation attack on stream ciphers[C]. In: International Workshop on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2006: 234–248.
[40] CARLET C, KHOO K, LIM C W, et al. Generalized correlation analysis of vectorial Boolean functions[C]. In: International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2007: 382–398.
[41] Biryukov A, De Cannière C, Quisquater M. On multiple linear approximations[C]. In: Advances in Cryptology—CRYPTO 2004. Springer Berlin Heidelberg, 2004: 311–325.
[42] HERMELIN M, CHO J Y, NYBERG K. Multidimensional linear cryptanalysis of reduced round Serpent[C]. In: Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 2008: 203–215.
[43] ZHANG B, LI Z, FENG D G, et al. Near collision attack on the grain v1 stream cipher[C]. In: International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2013: 518–538.
[44] ZHANG B, XU C, MEIER W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0[C]. In: Advances in Cryptology—CRYPTO 2015. Springer Berlin Heidelberg, 2015: 643–662.
[45] BERBAIN C, BILLET O, CANTEAUT A, et al. Sosemanuk, a fast software-oriented stream cipher[C]. In: New Stream Cipher Designs. Springer Berlin Heidelberg, 2008: 98–118.
[46] Zeng K, YANG C H, RAO T R N. On the linear consistency test (LCT) in cryptanalysis with applications[C]. In: Advances in Cryptology—CRYPTO 1989. Springer New York, 1990: 164–174.

作者信息

张斌(1976–), 研究员, 博士生导师. 主要研究领域为流密码的设计、分析及相关基础性数学问题.
E-mail: zhangbin@tca.iscas.ac.cn

徐超(1986–), 博士. 主要研究领域为流密码的安全性分析.
E-mail: xuchao@tca.iscas.ac.cn

冯登国(1965–), 研究员, 博士生导师. 主要研究领域为密码学.
E-mail: fengdg@263.net