流密码分析方法研究综述

周照存[1,2]，冯登国[1]

（1. 中国科学院软件研究所可信计算与信息保障实验室，北京 100190；2. 中国科学院大学，北京 100049）

摘 要：研究密码分析方法对设计密码算法至关重要。鉴于此，回顾了目前主要的流密码分析方法，研究了流密码分析方法的分类与联系，从主要技术特点的角度将其分为基于相关性质、差分性质、代数方程组和时间存储数据折中这 4 种类型，分别阐述了各分析方法的基本原理、主要技术及相关研究进展，并概括了其主要特点。此外，对流密码分析方法未来的发展方向进行了展望。

关键词：流密码；线性区分分析；相关分析；碰撞分析；立方分析；代数分析；猜测确定分析；时间存储数据折中分析

中图分类号：TN918.1

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022186

Survey on approaches of stream cipher cryptanalysis

ZHOU Zhaocun[1,2], FENG Dengguo[1]

1. Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
2. University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: Cryptanalysis plays an essential role in the design of ciphers algorithm. Based on this, the common approaches were reviewed and investigated to clarify their relations. These approaches were categorized into four classes according to their main techniques, i.e., the correlation-based approaches, the differentials-based approaches, the algebraic-equations-based approaches and the time-memory data trade-off (TMDTO) approaches. And their principles, basic technical ideas and developments were presented, and their main features were summarized. Moreover, the future of stream cipher cryptanalysis approach was prospected at last.

Keywords: stream cipher, linear distinguishing cryptanalysis, correlation cryptanalysis, collision cryptanalysis, cube cryptanalysis, algebraic cryptanalysis, guess-and-determine cryptanalysis, TMDTO cryptanalysis

0 引言

随着云计算、大数据、物联网等的发展和应用，具有快速、安全、轻量等特点的信息处理技术成为信息安全研究的重要需求。密码技术作为信息安全的核心技术，发挥着日益重要的作用。密码算法通常作为信息安全解决方案中的关键基元，其安全性、速率与资源占用等性质关系到整个方案的安全性与适用性。密码分析技术是设计安全、高效、轻量的密码算法中不可或缺的关键技术。

流密码算法是一类重要的对称密码算法，一般具有加解密效率高、实现简单等特点，因此应用广泛。一般来说，流密码算法由一个固定大小的内部状态，以及作用在该状态上的更新函数与输出函数组成。更新函数将前一时序的内部状态更新为下一时序的状态。输出函数则从内部状态中抽取信息以生成用于加解密的密钥流。

相对来说，流密码算法形式更为灵活，其常使用的密码构件有密码逻辑函数、移位寄存器以及常见的基本运算等。从上层结构看，常见的流密码包括线性

收稿日期：2022−07−07；**修回日期**：2022−09−13

基金项目：国家自然科学基金资助项目（No.U1636216）

Foundation Item: The National Natural Science of China (No.U1636216)

反馈移位寄存器（LFSR, linear feedback shift register），例如，ZUC 系列[1-2]、SNOW 系列[3-5]算法，还包括非线性反馈移位寄存器（NFSR, nonlinear feedback shift register），例如，Grain 系列[6-10]、Trivium[11]算法。更为详细的流密码分类可以参考文献[12-13]。

传统的流密码通常每个时序产生长为 1 bit 至数字节的密钥流。近年来，随着高速数据处理等新需求的出现，部分流密码也采用与分组密码构件组合设计的方式输出更长的密钥流，例如，SNOW-V[5]等算法以 AES 轮函数作为构件。从设计思想上看，这些算法与分组密码工作模式之间的边界更加模糊。

正因为流密码所呈现出的灵活多变的形式，流密码的分析方法也体现出多样化、专门化的特点。多样化是指不同分析方法所采用的关键技术与基本思想差异很大；专门化是指有些分析方法利用了流密码算法的特殊设计并对该类型的流密码算法更有效。根据安全模型的不同，可以将这些分析方法分为传统机密性分析和认证加密安全性分析。根据敌手能力的不同，可以分为唯密文分析、已知明文分析、选择明文分析和选择密文分析。根据密钥数量的不同，可以分为单密钥分析和多密钥分析。根据分析对象的不同，可以分为初始化分析、密钥流生成阶段分析和认证码生成阶段分析。根据分析结果的不同，可以分为区分分析和状态（密钥）恢复分析。根据数学工具的不同，可以分为确定性分析和统计性分析。

鉴于此，流密码分析方法的分类也是一个值得研究的课题。文献[14]回顾了部分流密码分析方法，但仅限于线性分析、相关分析方面的一些研究进展讨论，没有进一步阐述分析方法的理论细节。文献[15]将流密码的分析方法分为时间存储数据折中（TMDTD, time-memory data trade-off）类、相关分析类、线性分析类、代数分析类和猜测确定类，并结合具体流密码算法阐述了多种流密码分析方法。本文从主要技术特点的角度对流密码的主要分析方法进行分类研究，将现有的主要流密码分析方法分为基于相关性质的分析方法、基于差分性质的分析方法、基于代数方程组的分析方法和基于时间存储数据折中的分析方法 4 种，重点阐述分析方法本身的技术原理、所依赖的性质和相关公开问题，还涵盖了一些新的研究进展。这种分类方法与之前不同，更强调主要技术，有利于研究者把握流密码分析方法之间的区别和联系。例如，线性区分分析与相关分析被归为同一类，因两者都基于线性逼近技术；立方分析则被归为基于差分性质的分析方法，因其与高阶差分/积分分析技术有密切联系，故对利用划分性质改进立方分析显得非常重要；猜测确定分析则被归为基于代数方程组的分析方法，因为该方法实际上是从另一个角度求解代数方程组的。

1 基础知识

1.1 符号

$\oplus$ 表示异或，$\boldsymbol{xy}=\oplus_{i=1}^{m}x_iy_i$ 表示 2 个 m bit 向量的内积；$\boxplus$ 表示 2 个整数的模 2^n 加法；$\mathbb{F}_{2^n}$ 表示二元域的 n 次扩域；$\mathbb{F}_2[x]$ 表示系数在 $\mathbb{F}_2$ 上的多项式环；$\mathbb{B}_m$ 表示 m 个变元的布尔函数环；$\mathbb{Z}$ 表示整数环；$\mathrm{E}[X]$ 表示随机变量 X 的数学期望；$\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置矩阵。

1.2 基本定义

定义 1 线性反馈移位寄存器。一个 LFSR 一般包含 l 个寄存器单元 $(x_0,\cdots,x_{l-1})$ 和线性反馈关系 $x_l=c_1x_{l-1}+\cdots+c_lx_0$。

LFSR 有 2 种实现形式：Fibonacci 形式和 Galois 形式。2 种不同形式的 LFSR 在初态上相差一个线性变换。当反馈关系为非线性时，称之为 NFSR。

定义 2 线性逼近。令 Γ和Λ 分别表示 m bit 输入掩码和 n bit 输出掩码，一个 m 入 n 出的布尔函数 f 的线性逼近可表示为 $\Lambda\boldsymbol{y}\oplus\Gamma\boldsymbol{x}=e$，其中，$e$ 表示二元噪声变量。

一般地，当 Γ和Λ 分别表示 $\mathbb{F}_2$ 上的 $r\times m$ 和 $r\times n$ 矩阵时，称之为多维线性逼近。

定义 3 相关性与偏差。一个二元随机变量 e 的相关性定义为 $\mathrm{cor}(e)=\Pr(e=0)-\Pr(e=1)$，偏差则定义为 $\epsilon=\Pr(e=0)-\frac{1}{2}$。

线性逼近中的二元变量 e 的相关性简称为线性相关性。当噪声为向量时，一般采用平方欧几里得不平衡性（SEI, squared Euclidean imbalance）来度量其偏差。

定义 4 SEI。令 $\boldsymbol{e}\in\mathbb{F}_2^m$ 表示一个 m 维的随机向量，定义其概率分布的 SEI 为

$$\Delta(\boldsymbol{e})=2^m\sum_{x\in\mathbb{F}_2^m}\left(\Pr(\boldsymbol{e}=x)-2^{-m}\right)^2$$

Baigeneres 等[16]证明了 SEI 与线性相关性之间满足 $\Delta(\boldsymbol{e})=\sum_{\Gamma\neq 0}\mathrm{cor}^2(\Gamma\boldsymbol{e})$。这表明 m 维噪声的 SEI 可以分解为 2^m-1 个二元噪声相关性的平方和。

在研究线性相关性时，常用的一个工具是 Walsh 谱。

定义 5　Walsh-Hadamard 变换（WHT, Walsh-Hadamard transform）。令 $f:\{0,1\}^n \to \mathbb{Z}$ 表示一个 n 变元函数，其 WHT 定义为

$$\tilde{f}(s)=\sum_{x\in\{0,1\}^n} f(x)(-1)^{sx}$$

通过观察上述定义式右边可知，Walsh 谱 $\tilde{f}(s), s\in\{0,1\}^n$ 可以根据 Hadamard 矩阵的对称性质快速计算，所需时间复杂度为 $O(n2^n)$。这种计算方式称为快速 Walsh-Hadamard 变换（FWHT, fast Walsh-Hadamard transform）。

划分性质是立方分析中常用的概念，比特划分性质如定义 6 所示。

定义 6　比特划分性质[17]。假设 $\mathbb{X}$ 是一个元素在 $\mathbb{F}_2^n$ 中的多重集，$\mathbb{K}$ 是一个元素为 n bit 向量的集合，多重集 $\mathbb{X}$ 具有划分性质 $\mathcal{D}_{\mathbb{K}}^{1^n}$，如果它满足下列条件

$$\oplus_{\boldsymbol{x}\in\mathbb{X}}\boldsymbol{x}^{\boldsymbol{u}}=\begin{cases}\text{不定}, & \exists \boldsymbol{k}\in\mathbb{K}, \text{使}\boldsymbol{u}\succeq\boldsymbol{k}\\ 0, & \text{其他}\end{cases}$$

其中，$\boldsymbol{x}^{\boldsymbol{u}}=\prod_{i=1}^{n}x_i^{u_i}$，$\boldsymbol{u}\succeq\boldsymbol{k}$ 表示 $u_i>k_i,\forall i$。

2　基于相关性质的分析方法

本节阐述基于线性逼近相关性的流密码分析方法，主要包括线性区分分析和相关分析两类。线性区分分析与相关分析虽然理论方法不同，但都利用流密码算法有限状态自动机（FSW, finite state machine）输入与密钥流之间的线性相关性。这两类方法主要适用于使用 LFSR 构件的流密码算法。

2.1　线性区分分析

线性区分分析属于统计分析，其目标是将密钥流序列与随机序列区分开。Coppersmith[18]提出了一种流密码的线性区分分析方法，并应用该方法分析了 SNOW 2.0 算法的安全性。该方法利用分组密码中线性掩码传播技术来寻找流密码算法的 LFSR 状态与密钥流之间相关性较大的线性逼近关系，基本步骤如算法 1 所示。

算法 1　线性区分分析基本方法

输入　密钥流序列

输出　区分结果

/*预计算阶段*/

1) 寻找 LFSR 状态和密钥流之间相关性较大的线性逼近关系；

2) 寻找一个 LFSR 反馈多项式 $l(x)$ 的低代数次数、低汉明重量倍式 g，即 g 的代数次数不太大且项数很少（根据实际情况，通常取为 3 项或 4 项）；

3) 利用倍式 g 和堆积引理，建立关于密钥流的一个线性关系；

/*在线阶段*/

4) 利用关于密钥流的线性关系进行区分分析。

具体来说，设步骤 1)找到的线性逼近关系为

$$\left(\oplus_{i\in\mathcal{I}}x_{t+i}\right)\oplus\left(\oplus_{j\in\mathcal{J}}z_{t+j}\right)=e_t$$

联立 $|\mathcal{C}|$ 个线性逼近关系可得到关于密钥流的相关关系 $\oplus_{k\in\mathcal{C},j\in\mathcal{J}}z_{t+j+k}=\oplus_{k\in\mathcal{C}}e_{t+k}$，导出噪声 $\oplus_{k\in\mathcal{C}}e_{t+k}$ 的概率分布可以通过堆积引理得到。

在线阶段统计序列 $\oplus_{k\in\mathcal{C},j\in\mathcal{J}}z_{t+j+k}$ 中 0 和 1 的偏差，若偏差较大，则认为该密钥流是由流密码算法产生的；否则，认为是随机序列。

步骤 2)中寻找校验式可以归结为 k 子集和问题[19-21]。假设关于密钥流的线性关系的相关性为 cor，根据最优基本区分器的相关结论，步骤 4)所需的数据和时间复杂度都为 $O(\mathrm{cor}^{-2})$[16]。

Yang 等[22]应用有限域 $\mathbb{F}_{2^n}$ 上的区分分析方法分析了 SNOW 3G 算法。$\mathbb{F}_{2^n}$ 上的区分分析与前述方法的原理类似。注意到，相关性 cor 由 $|\mathcal{C}|$ 个二元噪声 e_{t+k} 的相关性堆积得到；而应用非二元域上的区分分析时，导出噪声是 $|\mathcal{C}|$ 个非二元噪声之和，故其概率分布由 $|\mathcal{C}|$ 个非二元噪声分布卷积得到。因此，导出噪声的 SEI 因卷积损失明显。为减少卷积损失，提高区分能力，要求 $g(x)$ 的系数都是1，但代价是 $g(x)$ 的代数次数升高了。

Yang 等[23]又提出有限域 $\mathbb{F}_p$ 上的线性区分分析方法并分析了 ZUC-256 算法，提出了谱值重合的启发式技术，以减少噪声卷积损失。

2.2　相关分析

相关分析是一种状态恢复分析，其基本原理是将流密码 LFSR 状态恢复问题转化为译码问题：将 LFSR 部分看作一个线性码，其中，初态视作信息位；将 LFSR 输出序列看作发送的码字；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。噪声信道一般选取二元对称信道（BSC, binary symmetric channel）。流密码输出的密钥流序列则可以看作所收到的码字，如图 1 所示。

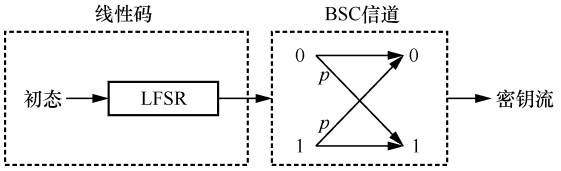

图 1 快速相关分析的二元信道译码模型

Siegenthaler[24]提出了对非线性组合生成器类型流密码的分别征服相关分析方法。其思想是利用组合函数的输入和输出之间的相关性，穷举搜索并恢复某个（或几个）特定 LFSR 的初始状态。这是最早的流密码相关分析方法。在此之后，流密码的相关分析得到了进一步发展，主要包含条件相关分析和快速相关分析两类分析方法。

2.2.1 条件相关分析

本节阐述 2 种条件相关分析方法，它们的共同点是利用条件相关性以获得更好的分析效果，区别是条件不同。

1) 基于输入相关性的条件相关分析

Lee 等[25]在 Anderson[26]提出的条件相关性思想的基础上，提出了一种条件相关分析方法。这种方法利用在特定输出条件下输入变量的相关性进行密码分析。由于条件相关性通常要比一般相关性更大，该方法可有效分析基于滤波生成器的流密码。该思想又被推广为混合相关分析和浓缩分析[27]。Lee 等提出的条件相关分析方法具体如算法 2 所示。

算法 2 Lee 等提出的条件相关分析方法

输入 密钥流序列

输出 LFSR 初态

1) 预计算条件相关性较大的输出模式集合 $D=\{\boldsymbol{y}\in\mathbb{F}_2^m \mid \lambda_f^m(\boldsymbol{y},\boldsymbol{c}_y)>p,\boldsymbol{c}_y\in\mathbb{F}_2^{n+m-1}\}$；

2) for i from 1 to l

3) 寻找密钥流序列中所有的 $\boldsymbol{y}\in D$；

4) 从 $\boldsymbol{c}_y$ 导出一个关于 LFSR 初态的线性方程；

5) end for

6) 从 l 个方程中随机选择 k 个求解，直到可以解出正确初态。

该方法原理如下。令 $f:\mathbb{F}_2^n\to\{0,1\}$ 表示非线性滤波函数，其中，f 的 m 次扩展函数记为

$$F^m:(x_1,\cdots,x_{n+m-1})\mapsto(f(\boldsymbol{x}_1),\cdots,f(\boldsymbol{x}_m))$$

其中，$\boldsymbol{x}_i=(x_i,\cdots,x_{i+n-1})$。定义

$$\lambda_f^m(\boldsymbol{y},\boldsymbol{c})=\left|\Pr\left(\boldsymbol{xc}=0|F^m(\boldsymbol{x})=\boldsymbol{y}\right)-0.5\right|$$

记 $\Lambda^m(f)=\max\lambda_f^m(\boldsymbol{y},\boldsymbol{c})$，因为 $\Lambda^m(f)$ 值随 m 增大而增大，所以若可以找到 $\Lambda^m(f)=\frac{1}{2}$，则可得到关于 LFSR 初态的线性方程。

由于 $\mathrm{E}[|\{\boldsymbol{x}|F^m(\boldsymbol{x})=\boldsymbol{y}\}|]=2^{n-1}$，预计算的时间复杂度为 $O(2^{2n+2m-2})$。当 n 较小时，可以通过穷举 $\boldsymbol{x}$、$\boldsymbol{c}$ 的方式计算集合 D；当 n 较大时，可以选择汉明重量较小的 $\boldsymbol{c}$ 来计算集合 D。对于大多数滤波函数，当 $n-2\leqslant m\leqslant n+2$ 时，条件相关性绝对偏差可达 0.45，因而预计算的时间复杂度约为 $O(2^{4n-2})$。

2) 基于输出相关性的条件相关分析

Lu 等[28]扩展了条件相关分析方法。该方法利用在部分输入未知且均匀随机的条件下，任意一个函数输出的条件相关性进行密码分析。这种条件相关性是前述输入条件相关性的反向推广，适用于敌手不仅可以看到密钥流，还可以访问由密钥部分控制的不确定的计算过程的场景。Zhang 等[29]进一步推广了计算条件相关性的函数。Lu 等提出的方法的原理如下。

令 $f:\mathbb{F}_2^u\times\mathbb{F}_2^v\to\mathbb{F}_2^r$，$f(B,X)=Z$ 表示一个双输入的布尔函数。当输入 B 给定时，记其为 $f_B(X)$。描述该相关分析的游戏和区分器如下。

游戏。预言机每次秘密独立随机地产生 (B,X)，用于计算 $f_B(X)$。敌手每次猜测 B，若猜测正确，则得到 $f_B(X)$，否则得到随机数 $Z_i^K\in\mathbb{F}_2^r$。最终得到 2^L 个长为 n 的序列（L 表示密钥的长度），其中只有一个序列为 $(f_{B_i^K}(X_i),B_i^K)$。敌手试图找出此序列。

区分器。猜测 2^L 个所有可能的密钥值，对于每一个猜测值 K，设一个权重 $G(K)$，其初值置 0。对于 n 个样本，累计计算

$$G(K)\leftarrow G(K)+\mathrm{lb}\left(2^r D_{f_{B_i^K}}\left(Z_i^K\right)\right)$$

以使 $G(K)$ 最大的猜测值 K 作为正确密钥候选值。

该区分器的数据复杂度为 $n=\frac{4L\ln 2}{\mathrm{E}[\Delta(f_B)]}$，但一般情况下的时间复杂度非常大。然而当 B_i^K、Z_i^K 满足特殊条件时，可以通过 FWHT 有效降低时间复杂度。蓝牙算法 E0 恰好满足此特殊条件，因而分析效果较好，而一般流密码算法并不具备这种性质，因而该条件分析方法应用较少。

2.2.2 快速相关分析

快速相关分析是一类非常重要的流密码分析方法。Meier 等[30]提出快速相关分析方法，以改进

分别征服相关分析中复杂度与 LFSR 长度呈指数关系的缺点。按照译码方式的不同，快速相关分析主要可以分为基于概率迭代译码的快速相关分析和基于硬判定译码的快速相关分析。

1) 基于概率迭代译码的快速相关分析

Meier 等[30]提出的译码算法（算法 B）是一种概率迭代译码算法，如算法 3 所示。译码算法的输入是一段长为 N 的连续密钥流 $z_t = x_t \oplus e_t$。若成功译码，则算法的输出为 x_t。

算法 3　概率迭代译码算法

输入　密钥流序列

输出　LFSR 初态

1) 计算概率阈值 p_{th} 和个数阈值 N_w;
2) 初始化所有位置的先验错误概率为 $p < 0.5$;
3) for 轮数从 1 至一个限定值 $R_{\max}$
4)　for 圈数从 1 至一个限定值 α
5)　　计算每个位置的后验概率 $p^* = \Pr(e_t = 0)$;
6)　if $p^* > p_{\text{th}}$ 的位置数$\geqslant N_w$ then break;
7)　else 置先验概率为后验概率;
8)　end if
9)　end for
10)　翻转所有 $p_t^* > p_{\text{th}}$ 的 z_t;
11)　if 序列满足 LFSR then 导出 LFSR 初态;
12)　else 重置所有先验概率为 p
13)　end if
14) end for

算法 3 中，概率阈值 p_{th} 和个数阈值 N_w 需要根据初始错误率 p、奇偶校验式成立的个数以及奇偶校验式抽头的个数由正态分布导出。后验概率 p^* 可根据贝叶斯公式导出，主要依据为：对于某个位置 $0 \leqslant t \leqslant N$，若观察到较多的校验式为 0，那么 p^* 应当增大。

Johansson 等[31-32]基于卷积码理论改进了译码方法。与之前方法相比，改进方法的校验式更容易生成。Canteaut 等[33]将 LDPC 码的译码方法应用到快速相关分析中，以使用汉明重量为 4 或 5 的校验式。Golic[34]提出了将编码理论中最优的逐符号译码算法 H-R 算法应用于快速相关分析，该方法可以利用非正交的校验等式。虽然理论上概率迭代译码的快速相关分析的译码能力更接近香农界，但基于此类译码方法的快速相关分析通常难刻画精确可靠的复杂度，因而很少应用于分析现实世界中的流密码算法。Zhou 等[35]将二元迭代译码算法推广至向量迭代译码算法，并分析了其部分理论复杂度。

2) 基于硬判定译码的快速相关分析

Chepyzhov 等[36]提出了一种基于信息集译码的快速相关分析方法。该方法通过折叠噪声来分析时间存储数据折中的复杂度，主要优势在于能够给出可靠的复杂度和成功概率理论估计。Johansson 等[37]提出了通过重建多项式的方法来进行快速相关分析，其基本原理与信息集译码方法相似，恢复对象由内部状态变为多项式。Mihaljevi 等[38]进一步提出可以用列表译码的方法进行快速相关分析。

Chose 等[39]提出通过构造关于密钥流数据的公开函数，并在预计算阶段对其进行 FWHT，避免校验式求值过程中的冗余计算。该方法大大提高了快速相关分析的效率，使快速相关分析成为分析基于 LFSR 的流密码最重要的方法之一。下面，阐述基于信息集译码和 FWHT 技术加速的快速相关分析的基本原理，如算法 4 所示。

算法 4　基于信息集译码和 FWHT 技术加速的快速相关分析

输入　密钥流序列

输出　LFSR 初态

/*预计算阶段*/

1) 寻找 LFSR 状态和密钥流之间的相关性较大的线性逼近关系;
2) 根据 LFSR 反馈关系和线性逼近，生成 M 个校验式。每个校验式在 $l - l'$ 个分量上取 0;

/*在线阶段*/

3) 构造关于密钥流的公开函数;
4) 计算公开函数的 Walsh 谱，根据最大绝对值谱值，先恢复 l' bit 内部状态;
5) 重复步骤 2)～步骤 4)，以更低的复杂度恢复剩余的状态。

具体来说，设 LFSR 的长度为 l bit，初态为 $\boldsymbol{s}^{(0)}$，t 时刻的状态为 $\boldsymbol{s}^{(t)}$，$\boldsymbol{A}$ 表示 LFSR 的生成矩阵，则线性逼近关系为

$$\boldsymbol{\Gamma}\boldsymbol{A}^t\boldsymbol{s}^{(0)} \oplus \left(\oplus_{j\in\mathcal{J}} z_{t+j}\right) = e_t$$

记 $\boldsymbol{g}^{(t)} = (\boldsymbol{\Gamma}\boldsymbol{A}^t)^{\mathrm{T}}$，可通过 k 子集和方法构造一些新校验式 $\boldsymbol{g}'^{(t)}$，满足在 $l - l'$ 个固定位置取 0[19-21]。类似地，折叠后 $\mathrm{cor}(e_t') = \mathrm{cor}(e_t)^k$，噪声 $z_t' = \oplus_{j\in\mathcal{J}} z_{t+j}$。

在线阶段根据 z_t' 构造译码函数 $w(\boldsymbol{x})$，并计算 Walsh 谱 $\tilde{w}(\boldsymbol{s})$。因为 Walsh 谱实际上表示经验相关性，且当猜测值正确时，经验相关性绝对值可能更大，故以 $|\tilde{w}(\boldsymbol{s})|$ 最大的 $\boldsymbol{s}$ 作为 $\boldsymbol{s}^{(0)}$ 的 l' bit。

算法 4 的复杂度主要受步骤 2)～步骤 4)的影响，译码所需的校验式个数 M 受码率不超过信道容量的限制。借助于 FWHT 加速，步骤 3)和步骤 4)所需复杂度由原来的 $O(M2^{l'})$ 降为 $O(M+l'2^{l'})$。

在预计算阶段，一般可以通过寻找线性路径的方式建立 LFSR 状态和密钥流之间的高相关性线性逼近关系。线性路径中线性掩码的传播与分组密码线性分析类似。因此，可以通过专门化算法或建立并求解自动化搜索模型的方式解决。

基于信息集译码快速相关分析方法已经很成熟，目前，研究者往往更专注在具体流密码中的应用。Zhang 等[40]将前述快速相关分析的方法推广到利用有限域上的线性逼近，改进了对 SNOW 2.0 算法的分析结果。Shi 等[41]使用 SMT/SAT 模型搜索了 SNOW-V 的高相关性线性逼近，并改进了快速相关分析结果。

Todo 等[42]提出快速相关分析方法，优势是可以同时降低时间和数据复杂度。该方法主要出发点是观察到 $\mathbb{F}_{2^m}$ 上线性掩码的乘法具备特殊交换性质。因此，在快速相关分析中可以考虑恢复中间状态而非初态，如算法 5 所示。

算法 5 Todo 等提出的快速相关分析方法

输入 密钥流序列

输出 LFSR 初态

/*预计算阶段*/

1) 寻找 LFSR 状态和密钥流之间的多个高相关性且密钥流掩码相同的线性逼近关系；

/*在线阶段*/

2) 绕过 β bit，构造关于密钥流的公开函数；

3) 计算公开函数的 Walsh 谱，保留所有的经验相关性大于某一阈值 $\mathrm{cor}_{\mathrm{th}}$ 的中间状态；

4) 对于步骤 3)保留的每个中间状态，尝试恢复正确的 LFSR 初态。

具体来说，设步骤 1)中共找到 m 个相关性为 $\mathrm{cor}(e)$ 的线性逼近，步骤 2)构造关于剩余 $(l-\beta)$bit 中间状态的译码函数并计算 Walsh 谱，该过程与算法 4 类似。记 ϵ_1 和 ϵ_2 分别表示正确和错误中间状态相关性大于阈值 $\mathrm{cor}_{\mathrm{th}}$ 的概率并设 2 种状态分别服从参数为 $\lambda_1 \approx m2^{-\beta}\epsilon_1$ 和 $\lambda_2 \approx m2^{-\beta}\epsilon_2$ 的泊松分布，只要 λ_1 相比 λ_2 较小，就可以筛选出正确初态。当 $N \approx (l-\beta)2^{l-\beta} \approx m2^{l-\beta}\epsilon_1$ 时，时间复杂度为 $O(3(l-\beta)2^{l-\beta})$，数据复杂度为 $O((l-\beta)2^{l-\beta})$。

在预计算阶段，同样可以通过建立并求解自动化搜索模型的方式寻找所需的线性逼近。特别地，当有限状态自动机由 NFSR 和滤波函数组成时，可以采用分析 NFSR 更新函数和滤波函数 Walsh 谱的方式，例如，Grain 系列算法。

此后，Wang 等[43]又证明了当有多条线性逼近时，校验式个数下界为 $\dfrac{4\pi\ln 2(l+1)}{m\mathrm{cor}^2(e)}$。这意味着当线性逼近较多时，所需的数据量更少。

2.3 小结

线性区分分析与相关分析都是针对密钥流生成阶段的分析方法。这类分析方法主要适用于基于 LFSR 的流密码算法。特别地，Todo 等[42]提出的快速相关分析方法适用于可以找到很多高相关性线性逼近关系，且不能够折叠噪声的情况。虽然大部分公开研究结果都是针对同步流密码的，但是该类分析方法建立在对数据的统计分析基础上，故理论上它们也适用于自同步流密码算法。在此情况下，线性掩码的传播应当同时考虑明文和密钥流。

与线性区分分析相比，快速相关分析需要考虑校验式快速求值问题，因此如何结合 FWHT 或 FFT 加速是分析的重要一环。这就要求所构造的译码函数谱值具有明确的现实意义。在非二元相关性质的快速相关分析中，这是一项具有挑战性的工作。

线性区分分析、条件相关分析、快速相关分析的一些典型分析应用如表 1 所示。值得注意的是，文献[42]中提出的快速相关分析方法也可以应用于分析 Plantlet 等类 Grain 轻量化流密码算法，但是复杂度折中关系有差别[43]，本文不再一一列举。

表 1 基于相关性质分析方法的部分典型应用

分析方法	分析对象	密钥长度/bit	分析效果（时间复杂度，数据复杂度，存储复杂度）
线性区分分析	SNOW 1.0	128	$2^{101.6}$, $2^{101.6}$, —
条件相关分析	E0	128	2^{39}, 2^{39}, —
快速相关分析	SNOW-V	256	$2^{246.53}$, $2^{237.5}$, $2^{238.77}$
	Grain-128a	128	$2^{115.4}$, $2^{113.8}$, —
	Grain-v1	80	$2^{76.7}$, $2^{75.1}$, —

对于基于相关性质的流密码分析方法，降低 FSM 的输入输出相关性是一种有效的防护手段，在

设计阶段就可以通过自动化搜索或人工推导的方式来分析最优化线性路径（逼近）的相关性。另外，增大 LFSR 的规模也是一种很有效的抵抗此类分析方法的防护手段。

目前，基于 $\mathbb{F}_{2^n}$ 上 LFSR 的流密码的线性区分方法已经较为成熟，而基于 $\mathbb{F}_{p\neq 2}$ 上 LFSR 的流密码的线性区分方法还面临 FSM 的线性逼近与 LFSR 数学结构不相容的问题。另外，由于多维线性逼近掩码空间更大，目前还没有有效的搜索方法。这是一些需要继续研究的问题。

基于信息集译码的快速相关分析技术目前已经较为完善，但几种条件相关分析应用局限性较强。如何改进条件相关分析方法以应用于分析现代流密码算法也是一个值得研究的具体课题。

基于相关性质流密码分析方法的特点如表 2 所示。

3　基于差分性质的分析方法

本节阐述基于差分性质的流密码分析方法，主要包括碰撞分析和立方分析。这两类方法主要适用于分析流密码算法的初始化过程或者认证流密码算法的认证码生成过程。

3.1　碰撞分析

3.1.1　差分分析

由于流密码的初始化过程类似于分组密码的轮迭代，因此可以采用分组密码的差分分析思想分析流密码的初始化过程。对于流密码，可利用初始向量（IV, initialization vector）对之间的输入差分与密钥生成阶段的输出差分性质构造区分器。文献[45]中研究了一般的（密钥，IV）差分对的差分特征，即 $(\Delta K,\Delta \mathrm{IV})\rightarrow \Delta s$。这种分析方法在原理上与分组密码的差分分析类似，本文不再展开阐述。

2007 年以后，差分分析方法的基本思想得到了推广，派生出选择 IV 分析方法[46-48]。通过选择 IV 的一个比特子集，并固定这个子集之外的 IV 变量和密钥变量，然后遍历该子集变量的所有可能取值，得到对应的所有的密钥流输出。这等效于生成以该子集变量为输入，以一个密钥流符号为输出的布尔函数真值表，并试图发现该函数的一些统计弱点。这种一般化的选择 IV 分析方法已经接近于后面将阐述的立方分析方法。

3.1.2　滑动分析

滑动分析基本思想源于分组密码滑动密钥分析。Biryukov 等[49]提出了滑动密钥分析，主要适用于分析轮对称性强的迭代型分组密码，随后被用于分析流密码算法初始化过程。滑动分析是一种多密钥分析，其基本思想是寻找一个密钥和初始向量对 (K,IV)，经过初始过程的数轮迭代后，流密码算法的内部状态恰好是另一对 (K',IV') 对应的初态，然后通过这种对称性质恢复出 K 或 K'。该方法与流密码算法的初始化轮数没有关系，主要利用部分流密码算法初始化过程中的对称性。

3.1.3　近似碰撞分析

Zhang 等[50]提出了近似碰撞分析，并用于分析 Grain-v1 算法。动机是观察到该算法 NFSR 和 LFSR 等长且 LFSR 独立更新，若 2 个时刻的内部状态仅相差很小，那么输出的密钥流片段彼此近似。根据近似生日碰撞原理，只要密钥流足够长，就可以找

表 2　基于相关性质流密码分析方法的特点

分析方法	主要技术	特点
线性区分分析	构造密钥流之间的线性相关性质	①适用于基于 LFSR 的流密码 ②受生成校验式和相关性的限制
Lee 的条件相关分析	输出条件下输入变量的相关性	①条件相关性强于一般相关性 ②适用于分析滤波函数型流密码
Lu 的条件相关分析	部分输入未知且均匀随机的条件下输出条件的相关性	①条件相关性强于一般相关性 ②特殊性质下 FWHT 加速 ③目前仅见于分析 E0 算法
Meier 的快速相关分析	基于贝叶斯迭代过程软判定噪声分布	①缺乏可靠的复杂度评估 ②受特殊校验式和相关性的限制
基于信息集译码的快速相关分析	基于噪声折叠技术多步状态恢复分析	①适用于基于 LFSR 的流密码 ②可 FWHT 加速计算 ③受生成校验式和相关性的限制
Todo 的快速相关分析	基于有限域上线性掩码的交换性先恢复中间状态	①可用多个线性逼近降低复杂度 ②可 FWHT 加速计算 ③受相关性和 LFSR 规模的限制

到内部状态上的近似碰撞。根据密钥流差分，检测出内部状态上的近似碰撞可以用于恢复 LFSR 状态。近似碰撞分析与时间存储数据折中分析有较密切的关联。下面，介绍其基本模型。

预计算阶段主要建立一些结构性的差分表。首先，穷举所有的汉明重量较小的内部状态差分，计算对应的所有密钥流差分。然后，为每个可能的密钥流差分建立一个表。每个表包含了所有可能产生该密钥流差分的内部状态差分，并将表中的内部状态差分按照所占比例进行排序。

在线阶段根据密钥流和预计算表提取内部状态的差分信息。因为 LFSR 独立更新，一旦得到正确的内部状态差分，就可以得到 LFSR 内部状态。

文献[50]还提出使用 BSW 采样技术改进近似碰撞。随后 Zhang 等[51]又对近似碰撞分析进行了改进，移除之前需要的假设，并将全状态的近似碰撞转换为部分状态的近似碰撞。

3.2 立方分析

立方分析最早由 Dinur 等[52]提出，是高阶差分分析的一种扩展，适用于更新函数代数次数较低的流密码算法。立方分析比较特殊，既可以是密钥恢复分析，也可以是区分分析。本节主要阐述传统立方分析、动态立方分析、基于划分性质的立方分析和条件立方分析。

3.2.1 传统立方分析

立方分析将初始化过程看作输入为初始变量 $\boldsymbol{v}$ 和密钥变量 $\boldsymbol{x}$、输出为第一比特密钥流 z 的一个布尔函数 $z=f(\boldsymbol{x},\boldsymbol{v})$。其后计算 f 的高阶差分得到简化的多项式，并用于恢复密钥或者建立区分器。具体来说，令 $f=t_I p_I \oplus q$，其中，I 是 $\boldsymbol{v}$ 下标索引的子集，t_I 是仅包含公开变量的单项式，p_I 不包含 $v_{i\in I}$ 中任何变量且 q 不能被 t_I 整除。因此可得 $\oplus_{\{v_{i\in I}\}} f = p_I$。一般将 $v_{i\in I}$ 中的变量称为立方变量，其余公开变量称为非立方变量。所有可能的立方赋值的集合 C_I 称为 d 维立方，p_I 称为 C_I 在 f 中的超级多项式。

立方分析包括预处理阶段和在线阶段。预处理阶段找到可以得到低次超级多项式的立方，并由此恢复出超级多项式。在线阶段通过询问加密预言机得到 z，再通过解低次方程组恢复一些密钥变量。

立方分析中有 2 个重要问题，一是选择合适的立方，二是测试超级多项式的线性或恢复超级多项式。对于后者，当攻击者把算法看作一个黑盒多项式时，在预处理阶段，可以使用随机测试法来确定给定的立方集超级多项式是否为线性并恢复超级多项式。

立方分析还可以用于区分流密码算法和随机函数，此时一般称为立方检验[53-54]。立方检验将 $\boldsymbol{v}$ 分成互补的两部分，即立方变量（CV）和超级多项式变量（SV）。通过选取特定的 CV 和 SV，检验超级多项式的性质，实现区分分析。常见的可用于立方检验的超级多项式性质有平衡性、常数函数、低次数、线性变量的存在性和变量退化等。

3.2.2 动态立方分析

Dinur 等[55]提出了动态立方分析。类似于立方分析，动态立方分析也是对立方变量遍历之后的输出结果求和。在立方分析和立方检验中，立方变量之外的所有公开变量设定为固定值，因此可称为静态变量；在动态立方分析中，某些非立方变量的值不是固定的，而是由定义在公开变量和秘密变量上的函数决定，称为动态变量。通常选取那些可以保持某些状态比特为 0 的函数，从而放大立方检验的非随机性。显然，动态立方分析是立方检验的推广和优化，攻击者能够直接推导密钥信息，不需要求解代数方程组。此外，选取适当的动态变量能够降低立方检验的时间复杂度（通常动态立方检验所需立方集的规模更小）。动态立方分析需要建立在对内部状态进行更加复杂的分析的基础上，基本原理如下。

假设一个多项式 P 可以分解为 $P=P_1P_2+P_3$，其中，P_1 为源多项式，P_2 为目标多项式，P_3 为剩余多项式。它们满足 P_2 是一个随机函数，P_3 是一个形式简单的函数，而 P_1 的形式为攻击者已知，则攻击者可以利用这些信息来获得密钥信息。例如，设 P_1 可以写成不同的项之和 $P_1=\sum_k t_{J_k\subseteq I}P_{1,k}+v_1$，其中，$t_{J_k\subseteq I}$ 表示立方集上的子项，$P_{1,k}$ 表示关于 $\boldsymbol{x}$ 的多项式，$P_{1,k}$ 之间的公共变量较少。那么攻击者将 v_1 设为动态变量，令其为 $v_1=\sum_k t_{J_k\subseteq I}P_{1,k}$。由于 $P_{1,k}$ 未知，攻击者猜测 $P_{i,k}$ 所有可能的 2^k 个取值。如果猜测正确，则对此赋值，$P=P_3(v_1=\sum_k t_{J_k\subseteq I}P_{1,k})$ 具有较简单的形式，因而进一步将立方检验与随机函数区分开，并可以由此推导密钥的信息。如果猜测错误，则大概率 $P_1\neq 0$，这时 $P=P(v_1=\sum_k t_{J_k\subseteq I}P_{1,k})$ 的形式近似于随机，因而不能与随机多项式区分。

3.2.3 基于划分性质的立方分析

划分性质是 Todo[17]提出的一种寻找分组密码高

阶差分（积分）特征的新技术。随后，基于比特级的划分性质被提出并应用于多个算法的分析中[56]。文献[56-58]提出了划分性质的一些传播法则。自立方分析提出以来，立方的大小一直受实验限制。这种情况一直到 Todo 等[57]提出利用划分性质分析代数正规型的系数来恢复超级多项式的方法后才得到改观。计算划分性质的传播并不容易，Xiang 等[58]通过混合整数线性规划（MILP, mixed-integer linear programming）有效地计算了划分性质的传播。

记 $f=\oplus_{\boldsymbol{u}\in\mathbb{F}_2^n} a_{\boldsymbol{u}}^f \boldsymbol{x}^{\boldsymbol{u}}$，其中，$a_{\boldsymbol{u}}^f\in\mathbb{F}_2$ 为代数正规型的系数。记 $\boldsymbol{k}$ 为一个 n 维的比特向量，若不存在 $\boldsymbol{k}$ 到 1 的划分迹，则对任意的 $\boldsymbol{u}\succeq\boldsymbol{k}$ 都有 $a_{\boldsymbol{u}}^f=0$。基于此，Todo 等给出了利用划分性质和 MILP 恢复超级多项式 $p_I(\boldsymbol{x},\boldsymbol{v})$ 的算法，如算法 6 所示。

算法 6　基于 MILP 估计超级多项式中的秘密变量

输入　MILP 模型 $\mathcal{M}$，指标集 I

输出　集合 J

1) 设 $\boldsymbol{x}$ 是 MILP 变量的 m 个秘密变量，$\boldsymbol{v}$ 是 n 个公开变量；$J=\varnothing$；

2) $\mathcal{M}$ 中添加约束：对任意的 $i\in I$，$v_i=1$；

$\forall i\in\{1,2,\cdots,n\}-I$，$v_i=0$；$\sum_{i=1}^{m} x_i=1$；

3) while $\mathcal{M}$ 有可行解

4)　　选择一个 $j\in\{1,2,\cdots,m\}$，使 $x_j=1$；

5)　　$J=J\bigcup\{j\}$；$\mathcal{M}$ 中添加约束：$x_j=0$；

6) end while

7) 返回 J

利用算法 6 分析超级多项式可知，只有 $x_j(j\in J)$ 与立方集 C_I 对应的超级多项式有关。攻击者选择 IV 的常数部分为某一固定常数并得到一个立方集 C_I，随后通过组合所有可能的秘密变量来恢复超级多项式，其时间复杂度为 $O(2^{|I|+|J|})$。

Wang 等[59]提出了 Flag 技术，进一步改进了立方分析 MILP 模型的精确性。改进的模型能够识别那些可得到非常数超级多项式的非立方变量赋值。同时，还改进了对于超级多项式项数的估计。Wang 等[60]采用三子集可分性的概念改进了求超级多项式的算法，并降低了时间复杂度。Hao 等[61]提出了基于完善的三子集的多重集合的可分性定义，使 MILP 模型在计算超级多项式时更准确，同时也回答了如何准确恢复超级多项式的问题。Sun[62]回答了如何搜索好的立方的问题，并给出了启发式的自动化搜索算法。所谓好的立方是指其对应的超级多项式至少有一个平衡的秘密变量。同时，Sun 基于此算法改进了 Hao 等对 Trivium 算法的分析结果。目前，基于划分性质的立方分析是一个研究热点。

3.2.4　条件立方分析

Huang 等[63]提出了条件立方分析。条件立方分析一般针对基于 Sponge 结构的 Keccak-MAC 及类似密码算法。该方法受动态立方分析方法的启发，试图通过增加对 IV 的条件来降低立方变量多项式的次数。这种技术与消息修改技术[64]和条件差分分析[65]有类似之处，也是通过一些比特条件来控制差分传播。基于这些条件的立方测试器一般被称为条件立方测试器。Li 等[66]推广了此方法并用于 Ascon 认证加密算法的分析。下面，简单阐述 Li 等的方法。

假设一个类 Keccak-MAC 算法一次输出 l bit。每 1 bit 输出可以写成秘密变量和公开变量的布尔函数 $f_i(\boldsymbol{x},\boldsymbol{v})$，$0\leqslant i<l$。选择一个公共立方 C_I，将 f_i 重写为 $f_i=t_IP_i+Q_i$。在条件立方分析中，寻找多项式 P_i 的公因子，即 $P_i=gP_i'$，因此，当立方求和后得到 $\sum_{C_I} f_j=gP_i'$。如果公因式 g 的形式足够简单，如 $g=x_0$，则可以采用立方测试器确定 x_0。

3.3　小结

本节所阐述的基于差分性质的分析方法都是分析流密码算法初始化过程，因而对于自同步流密码也适用。差分分析是一种一般化的分析方法，对初始化过程扩散混淆性质较弱的流密码效果较好。滑动分析则仅适用于初始化迭代对称性强的流密码算法。近似碰撞分析则适用于具有紧凑的 NFSR-LFSR 型流密码算法。立方分析针对初始化阶段的代数性质，目标是构造立方区分器和恢复密钥。目前，立方攻击主要适用于更新函数简单的轻量级流密码。而基于字的流密码一般采用代数次数和扩散性较强的更新函数，因而，立方分析应用较少。表 3 列出了基于差分性质分析方法的部分典型应用。

对于差分分析、滑动分析的防护设计已经较为成熟，通过增强更新函数密码性质、引入初态常数

表 3　　**基于差分性质分析方法的部分典型应用**

分析方法	分析对象	密钥长度/bit	分析效果（T 为时间复杂度，D 为数据复杂度）
差分分析	Helix	256	$T=2^{88}, D=2^{12}$ [67]
滑动分析	Grain v0	80	2^{-2} 概率滑动碰撞[68]
近似碰撞分析	Grain-v1	80	$T=2^{86.1}, D=2^{19}$ [51]
传统立方分析	767 轮 Trivium	128	$T=2^{36}$ [52]
动态立方分析	全轮 Grain-128	128	弱密钥集上快于穷举[55]
	全轮 Grain-128	128	选择 IV 假设 $T=2^{84}, D=2^{62.4}$
划分性质立方分析	855 轮 Trivium	80	$T=2^{77}$ [62]
	190 轮 Grain-128AEAD	128	$T=2^{123}$ [61]
	763 轮 Acorn	128	$T=2^{125.54}$ [69]
条件立方分析	Ascon	128	$T=2^{1039}$ [66]
	容量 256/512Keccak-MAC	128	$T=D=2^{72}$ [63]

可以较为有效地抵抗此类分析。由于近似碰撞分析与时间存储数据折中分析有关联，且利用了密钥流差分与内部状态差分之间的近似性，因此合理地增大出口函数规模和内部状态规模（含轮密钥）可以增强近似碰撞分析的安全性。

值得注意的是，立方分析与 MILP 方法结合后突破了之前仅能使用小立方集的限制，实现了更大的立方集搜索和更多轮数的区分器。一方面，尽管更复杂的更新函数和更多的初始化轮数有助于抵抗立方分析，但在公开轻量级流密码设计中，更新函数和初始化轮数是需要平衡的重要设计指标。另一方面，近年来，立方分析技术在不断进步。因此，立方分析在轻量级流密码的分析与设计中还将会发挥很大作用，并不断发展。

表 4 简单总结了基于差分性质流密码分析方法的特点。各种立方分析的基本思想类似，但技术细节有所不同。

4　基于代数方程组的分析方法

本节阐述基于代数方程组的流密码分析方法。该类分析方法都是通过求解代数方程组来恢复内部状态，但求解策略有所不同。一种方式是猜测可能的原象，根据函数值验证正确性，即猜测确定分析；另一种方式是通过数学理论求解方程组得到原象，即代数分析。

4.1　猜测确定分析

Knudsen 等[70]在分析 RC4 时提出了猜测确定分析的思想。Pasalic[71]提出了针对过滤生成器的猜测确定分析方法。

猜测确定分析的基本思想是将流密码内部状态划分为 2 个集合：猜测集合和确定集合。攻击者穷举猜测集合状态可能值，然后利用该部分内部状态值来求得确定集合内部状态。最后，攻击者还需将算法输出和密钥流进行比较，以检验猜测的正确

表 4　　**基于差分性质流密码分析方法的特点**

分析方法	主要技术	特点
差分分析	与分组密码差分分析相似	受差分传播性质制约
滑动分析	与滑动密钥分析相似	受轮对称性制约
近似碰撞分析	基于内部状态近似差分与密钥流差分的不均匀性	受算法结构影响大
传统立方分析	通过计算公开变量高阶差分来简化多项式以恢复秘密变量或者建立区分器	要求初始化更新函数简单
动态立方分析	部分公开变量设为动态以放大立方检验的非随机性	①所需立方集的规模更小 ②内部状态分析更加复杂
划分性质立方分析	基于划分性质分析代数正规型的系数来恢复超级多项式	①实现了更大的立方集 ②能够有效恢复超级多项式
条件立方分析	通过增加对 IV 的条件来降低立方变量多项式的次数	适用于类 Keccak-MAC 算法

性。因此，猜测确定分析的目标是寻找更小的猜测集，并以较少的复杂度来得到确定集合状态。

Feng 等[72]利用猜测确定方法分析了 SOSEMANUK。根据 SOSEMANUK 特殊的反馈多项式，改进为面向字节而非 32 bit 字的猜测确定分析。Yang 等[73]提出了 D 方程技术以改进猜测确定路径，并改进了对 SNOW-V 算法的分析结果。下面，简单阐述其基本原理。

一条猜测路径是指所有有序的猜测并由此确定的变量元组。如果能够以合理的顺序猜测这些变量，则有可能猜测量更少或者截断那些包含了不能满足中间代数方程的已知猜测值。在猜测确定的中间过程中，如果要求所有的解都要满足一些限定条件或者方程，则可以利用一些特殊的枚举方法（如递归枚举算法等）来代替直接的循环穷举。

接下来，举例说明 Yang 等利用 D 方程截断猜测路径的技术。令 $A=B\boxplus(C\oplus X)\boxplus(X\oplus D)$ 表示第一类 D 方程。设 A,B,C,D 是 n bit 变量且服从均匀分布，而 X 的值未知。首先，计算出 X 的解数量分布表。设上述 D 方程存在解的概率为 2^{-r}，那么对于所有可能的猜测值 A,B,C,D 组合，平均只有 $|(A,B,C,D)|2^{-r}$ 个组合是合法的。由此，就可以在中间过程中去掉不合法的猜测组合，而不必遍历并验证 (A,B,C,D) 所有可能值。

4.2　代数分析

代数分析最初应用于公钥和分组密码中。Courtois 等[74]将其应用于分析流密码 Toyocrypt 和 LILI-128。传统代数分析的基本思想是将流密码视作多变元函数，建立关于内部状态和密钥流之间的超定非线性方程组，再通过求解代数方程组的数学技术来恢复内部状态。例如

$$\begin{cases} z_0 = f(A^0(k_1,\cdots,k_n)) \\ \vdots \\ z_N = f(A^N(k_1,\cdots,k_n)) \end{cases}$$

其中，A 表示 LFSR 的更新变换。代数分析中建立并求解大规模非线性方程组的复杂度通常较大。

在求解代数方程组方面，目前的方法主要有 Gröbner 基法[75]、再线性化法[76]、XL（extensible language）法[76]、XSL（extensible style sheet language）法[77]等。代数次数是非线性方程组求解中的重要影响因素。注意到，将布尔函数 f 与另一个合理选择的布尔函数 g 相乘，有可能大大降低 f 的代数次数。文献[78]将其概括为代数免疫度的概念。对于变量数量较多的一般布尔函数，目前仍无有效的代数免疫度计算方法。布尔函数的代数免疫性质是代数分析中需要进一步研究的课题。

另外一个研究课题是如何建立并使用低次数多变元非线性方程组。不同的代数分析方法使用的代数方程类型一般不同，获得方程的技术也有所差别。下面，本节简单阐述一种使用双层甲板方程的快速代数分析的原理[74]。该方法可利用如下形式的代数方程

$$L(A^t(k_1,\cdots,k_n)) = R(A^t(k_1,\cdots,k_n),z_1,\cdots,z_m)$$

其中，L 是关于密钥的代数次数小于或等于 d 次的多项式，R 是关于密钥和密钥流比特的多项式，满足每项中密钥变量的代数次数不超过 d，密钥流变量的代数次数不超过 2。快速代数分析需在预计算阶段生成约 C_n^d 个此类方程。当密钥流连续（或等间隔）且 LFSR 是周期的时，前述代数方程即可按时序 t 迭代下去，以生成更多的方程。

设已找到 $S\leqslant\mathrm{C}_n^d$ 个代数方程，下一步希望找到线性组合关系 $0=\sum_{i=0}^{S-1}c_iL\sum_{i=0}^{S-1}c_iR$。快速代数分析将 $L(A^t(k_1,\cdots,k_n))$ 看作一个滤波函数型流密码算法，对其输出 $a_t=L(A^t(k_1,\cdots,k_n))$ 应用 B-M（Berlekamp-Massey）算法来解决此问题，具体介绍如下。

第 1 步：选择一个随机密钥，生成 $2S$ 长的序列 a_t，$0\leqslant t\leqslant 2S-1$。

第 2 步：应用 B-M 算法，得到 a_t 的一个反馈关系，将其作为 c_i，$0\leqslant i\leqslant S-1$。

得到足够多的方程 $\sum_{i=0}^{S-1}c_iR=0$ 后，可以通过计算低次零化子并结合 XL 等方法求得密钥 $k_1,\cdots,k_n$。

以上过程中，B-M 算法的时间复杂度为 $O(S\mathrm{lb}S+Sn)$，求解代数方程组的复杂度则由具体求解算法给出。

Armknecht[79]证明了预计算过程的合理性，并改进了预计算方法。Braeken 等[80]提出概率代数分析方法，允许方程以低于 1 的概率成立，但仅考虑了概率代数分析的应用可能性。如何求解大规模概率非线性方程组仍然是个公开问题。

4.3　小结

猜测确定分析是一类一般化的流密码分析方

法，可以应用于分析不同类型的流密码。快速代数分析方法主要适用于滤波函数型流密码算法，或者 FSM 中记忆单元很少的流密码算法。相比于代数分析，快速代数分析改进了代数方程的生成方式，但是对密钥流的要求提高了。

表 5 给出了基于差分性质分析方法的部分典型应用。

表 5 基于差分性质分析方法的部分典型应用

分析方法	分析对象	密钥长度/bit	时间复杂度
猜测确定分析	SOSEMANUK	128	2^{176} [72]
	SNOW-V	256	2^{378} [73]
代数分析	LILI-128	128	2^{57} [74]
	Toyocrypt	128	2^{49} [74]
快速代数分析	E0	128	2^{49} [80]

公开流密码算法在设计上一般采用较大的状态，并结合自动化搜索等方式评估内部状态之间的依赖性，以提高抵抗猜测确定分析的能力。而增强 FSM 更新函数的性质（如代数次数）并结合较大规模的 FSM 状态，可增强抵抗代数分析类方法的能力。

目前，猜测确定分析最优猜测集的选取是一个值得研究的课题。近年来，采用自动化搜索技术（如 MILP 建模）搜索最优猜测集的技术发展很快，往往可以获得更优更精细的结果。对于现代流密码来说，单纯地猜测确定分析、代数分析的分析效果可能不能令人满意，但这些技术与其他分析方法结合使用有可能得到更好的分析结果。这是代数分析和猜测确定分析中一个值得研究的课题。

表 6 简单总结了基于代数方程组流密码分析方法的特点。

表 6 基于代数方程组流密码分析方法的特点

分析方法	主要技术	特点
猜测确定分析	依据状态更新间的依赖关系	①具有一般性 ②受状态大小及状态依赖关系影响较大
快速代数分析	B-M 算法建立方程	①对滤波型或记忆单元少的流密码效果好 ②可求解性受代数次数、变量数量等影响

5 基于时间存储数据折中的分析方法

时间存储数据折中分析方法最早由 Hellman[82] 提出并应用于分析分组密码算法。随后 Biryukov 等[83] 将此方法用于分析流密码，也称为 BSW 时间存储数据折中分析，其基本原理如下。

令 N 表示内部状态大小，P 表示预计算阶段时间，M 表示存储空间大小，T 表示在线阶段时间，D 表示数据量大小，f_i 表示从内部状态到密钥流前缀的函数，目标是建立一个离线表以尽可能大地覆盖内部状态空间。因为对于流密码算法，部分重叠的密钥流前缀并不意味着内部状态也相邻，所以可以把内部状态看作随机点。如果 D 个前缀中有一个可以在离线表中找到，则可以回溯表中的那条链以恢复内部状态。因此，离线表需要覆盖的空间大小变为 $\frac{N}{D}$。同时，若 Hellman 时间存储数据折中离线表中包含 t 个 $m\times t$ 的矩阵，且满足生日终止规则 $mt^2=N$，在 TMDTO 中，矩阵大小不变，但数量变为 $\frac{t}{D}(t\geqslant D)$，因此仍然满足 $mt^2=N$。由于每个矩阵大小仍然为 $m\times t$，但数量减少了，因此存储空间大小降低为 $M=\frac{mt}{D}$，预计算的时间也降低为 $P=\frac{N}{D}$。根据生日终止规则，可以得到新的折中曲线 $TM^2D^2=N^2$。

为了避免在线阶段频繁查询离线表，在 TMDTO 方法中引入特殊点技术，即只有迭代生成特殊点时才查询离线表，但折中曲线仍然不变。同时，可以采用 BSW 采样技术，使 T 的选择更加灵活[84]。BSW 采样的基本思想是在很多流密码中，在输出下一比特密钥流前，内部状态更新有限。因此，就可以找到所有的能够生成 k bit 全 0 密钥流的特殊状态。若流密码内部状态大小为 $N=2^n$，即内部状态共 n bit，则称每个特殊状态有一个 $(n-k)$ bit 的缩略名。由此可以导出一个从内部状态到密钥流的随机映射，此时折中曲线仍然不变。

Maitra 等[85]提出可以通过固定一些比特以更容易地得到特殊状态，并可以通过密钥流导出部分内部状态值，但是该方法会增加数据量。

相比其他分析方法，时间存储数据折中分析方法是一类一般化的分析方法，它将流密码算法看作一个黑盒，并不注重算法逻辑。该分析方法的复杂度度量单位可以是一次加密，因而受算法的工作效率影响很大。

时间存储数据折中分析方法的典型应用包括对轻量级算法 Sprout、Lizard 等的分析，如表 7 所示。值得注意的是，对于 Sprout 算法的分析，尽管

该算法采用了 2 种状态：内部状态和密钥状态，但是仍然不能抵抗 TMDTO 分析。

表 7　基于时间存储数据折中分析方法的部分典型应用

分析方法	分析对象	密钥长度/bit	分析效果（预计算复杂度，在线计算复杂度）
时间存储数据折中分析	Lizard	60	2^{67}, 2^{54} [85]
	Sprout	80	$2^{41.3}$, 2^{40} [86]

为了防护 TMDTO 分析，公开非轻量流密码算法一般遵循“内部状态大小至少是密钥长度的 2 倍”准则。

虽然 Sprout 算法不能抵抗 TMDTO 分析，但后来设计的一些小状态轻量级流密码算法吸取有关设计经验，采用了一些特殊的设计，也声称具有良好的抵抗 TMDTO 分析的效果。这类算法的分析是一个值得思考的问题。

表 8 总结了基于时间存储数据折中的流密码分析方法的特点。

表 8　基于时间存储数据折中的流密码分析方法的特点

分析方法	主要技术	特点
基于时间存储数据折中的流密码	建立大规模离线表有关技术	①具有一般性 ②受内部状态大小（或密钥是否参与更新）影响很大

6　未来研究展望

流密码分析方法已经历了几十年的发展，至今仍在不断更新完善。回顾其发展历程，注意到近年来的流密码分析方法研究呈现出一些特点。这些特点可能会进一步影响未来一段时间流密码分析方法的发展。

1) 寻找新的密码性质，改进流密码分析方法。从流密码分析方法发展过程中可以发现，每当有可利用的新性质时，流密码的分析方法都会快速发展。因此，寻找新的密码性质，改进流密码分析方法仍然是重要的研究方向。例如，Todo 等[42]发现了线性掩码在限域上的交换性，并利用这种性质提出了一种新的快速相关分析方法。这类研究需要建立在对流密码分析方法深刻理解和细致观察的基础上。

2) 发掘不同密码分析技术之间的关联性，改进流密码分析方法。不同的密码分析方法采用不同技术对同一密码算法进行分析，这些分析方法之间可能存在联系。这种联系已经在分组密码分析方法中被发现，并得到了大量研究，例如，分组密码不可能差分分析、积分分析、零相关分析等方法之间的联系。在流密码分析中的一个典型例子是立方分析。一方面，自立方分析提出后，立方分析主要受限于实验规模对立方大小的限制[52]。另一方面，Todo[17]提出了针对分组密码的基于划分性质的广义积分分析，随后 Xiang 等[58]提出了划分迹的概念并将 MILP 技术引入划分性质的传播评估中。注意到，立方分析与积分分析技术具有密切联系，Todo 等[57]将划分性质引入立方分析中，并结合 MILP 技术用于恢复超级多项式。这是立方分析的一个里程碑式的发展。因此，发掘不同密码分析技术之间的关联性，对于改进现有流密码分析方法具有重要作用。这可能是流密码分析的一个突破方向。

3) 改进自动化搜索建模技术，提高流密码分析效果。目前，将流密码分析中的问题转化为 MILP 模型或 SAT/SMT 模型，寻求高质量解的技术在流密码分析中的应用越来越广泛。例如，应用于相关分析中寻找好的线性逼近关系[87]，应用于立方分析中恢复超级多项式[57]，应用于猜测确定分析中寻找好的猜测集[88]等，同时密码分析中的需求也促进了 MILP 建模技术的发展[89]。可以说，流密码分析方法与自动化分析技术结合越来越紧密。目前，一般通过约束关系刻画具体流密码算法中运算环节的密码性质的方式建立模型。例如，刻画 S 盒的线性逼近分布表。因此，建立更加精确的自动化模型，优化已有的分析方法仍然是一个值得研究的方向。

4) 组合使用多种流密码分析技术。近年来，有些流密码的分析已不再局限于单一方法，往往在一个算法的分析中组合使用多种分析技术。例如，猜测确定分析与线性分析和中间相遇的组合使用[90]、中间相遇与立方分析的结合[91]等。

5) 探索建立关于流密码分析方法更深刻的理论。Beyne[92]提出了线性分析的几何方法理论。该理论给出了常见的分组密码线性分析技术及其变体的统一描述，例如，一般线性分析、多维线性分析、不变子空间分析、非线性不变量分析等分析方法和技术。这种数学化的刻画对深刻认识线性分析的基础和不同分析方法之间的内在联系具有重要作用。一些流密码分析技术与分组密码分析技术之间具有密切的联系。建立类似的理论也将是流密码分析方法发展过程中的重要进展。

综上所述，流密码分析方法方面还有很多值得研究的方向[93-95]。未来，还需要研究者不断加深对

流密码分析的认识，以创新流密码分析方法。

7 结束语

研究流密码分析方法不仅可以促进密码分析技术的进步，对设计安全、高效的流密码算法也具有重要的指导价值。流密码分析方法种类多，差异明显。本文对目前常见的流密码分析方法按照技术特点的不同进行了分类汇总，并阐述了 4 大类 10 余种流密码分析方法的基本原理、主要技术以及研究进展。同时，也对流密码分析方法进行了展望。

参考文献：

[1] 冯秀涛. 3GPP LTE 国际加密标准 ZUC 算法[J]. 信息安全与通信保密, 2011, 9(12): 45-46.
FENG X T. ZUC algorithm: 3GPP LTE international encryption standard[J]. Information Security and Communications Privacy, 2011, 9(12): 45-46.

[2] TEAM D. ZUC-256 流密码算法[J]. 密码学报, 2018, 5(2): 167-179.
TEAM D. ZUC-256 stream cipher[J]. Journal of Cryptologic Research, 2018, 5(2): 167-179.

[3] ETSI/SAGE. Specification of the 3GPP confidentiality and integrity algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification[S]. 2006.

[4] EKDAHL P, JOHANSSON T. A new version of the stream cipher SNOW[C]//Selected Areas in Cryptography. Berlin: Springer, 2002: 47-61.

[5] EKDAHL P, JOHANSSON T, MAXIMOV A, et al. A new SNOW stream cipher called SNOW-V[J]. IACR Transactions on Symmetric Cryptology, 2019(3): 1-42.

[6] HELL M, JOHANSSON T, MEIER W. Grain: a stream cipher for constrained environments[J]. International Journal of Wireless and Mobile Computing, 2006, 2(1): 86-93.

[7] AGREN M, HELL M, JOHANSSON T, et al. Grain-128a: a new version of Grain-128 with optional authentication[J]. International Journal of Wireless and Mobile Computing, 2011, 5(1): 48-59.

[8] HELL M, JOHANSSON T, MEIER W, et al. An AEAD variant of the grain stream cipher[C]//Codes, Cryptology and Information Security. Berlin: Springer, 2019: 55-71.

[9] ARMKNECHT F, MIKHALEV V. On lightweight stream ciphers with shorter internal states[C]//Fast Software Encryption 2015. Berlin: Springer, 2015: 451-470.

[10] MIKHALEV V, ARMKNECHT F, MULLER C. On ciphers that continuously access the non-volatile key[J]. IACR Transactions on Symmetric Cryptology, 2016(2): 52-79.

[11] CANNIERE C, PRENEEL B. Trivium[C]//New Stream Cipher Designs. Berlin: Springer, 2008: 244-266.

[12] JIAO L, HAO Y L, FENG D G. Stream cipher designs: a review[J]. Science China Information Sciences, 2020, 63(3): 1-25.

[13] 赵石磊, 刘玲, 黄海, 等. 流密码算法、架构与硬件实现研究[J]. 密码学报, 2021, 8(6): 1039-1057.
ZHAO S L, LIU L, HUANG H, et al. Algorithm, architecture and hardware implementation of stream cipher[J]. Journal of Cryptologic Research, 2021, 8(6): 1039-1057.

[14] 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.
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.

[15] 冯登国. 序列密码分析方法[M]. 北京: 清华大学出版社, 2021.
FENG D G. Stream cipher cryptanalysis approaches[M]. Beijing: Tsinghua University Press, 2021.

[16] BAIGENERES T, JUNOD P, VAUDENAY S. How far can we go beyond linear cryptanalysis[C]//Advances in Cryptology - ASIACRYPT 2004. Berlin: Springer, 2004: 432-450.

[17] TODO Y. Structural evaluation by generalized integral property[C]//EUROCRYPT 2015. Berlin: Springer, 2015: 287-314.

[18] COPPERSMITH D, HALEVI S, JUTLA C. Cryptanalysis of stream ciphers with linear masking[C]//Annual International Cryptology Conference. Berlin: Springer, 2002: 515-532.

[19] NIKOLIC I, SASAKI Y. Refinements of the k-tree algorithm for generalized birthday problem[C]//Advances in Cryptology-ASIA CRYPT 2015. Berlin: Springer, 2015: 683-703.

[20] WAGNER D. A generalized birthday problem[C]//Advance in Cryptology - CRYPTO 2002. Berlin: Springer, 2002: 18-22.

[21] MINDER L, SINCLAIR A. The extended k-tree algorithm[J]. Journal of Cryptology, 2012, 25(2): 349-382.

[22] YANG J, JOHANSSON T, MAXIMOV A. Vectorized linear approximations for attacks on SNOW 3G[J]. IACR Transactions on Symmetric Cryptology, 2020(4): 249-271.

[23] YANG J, JOHANSSON T, MAXIMOV A. Spectral analysis of ZUC-256[J]. IACR Transactions on Symmetric Cryptology, 2020(1): 266-288.

[24] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, 34(1): 81-85.

[25] LEE S, CHEE S, PARK S, et al. Conditional correlation attack on nonlinear filter generators[C]//Advances in Cryptology-ASIACRYPT'96. Berlin: Springer, 1996: 360-367.

[26] ANDERSON R. Searching for the optimum correlation attack[C]//Fast Software Encryption 1995. Berlin: Springer, 1995: 137-143.

[27] LÖHLEIN B. Attacks based on conditional correlations against the nonlinear filter generator[J]. IACR Cryptology ePrint Archive, 2003, 2003: 20.

[28] LU Y, MEIER W, VAUDENAY S. The conditional correlation attack: a practical attack on bluetooth encryption[C]//Advances in Cryptology - CRYPTO 2005. Berlin: Springer, 2005: 97-117.

[29] ZHANG B, XU C, FENG D G. Real time cryptanalysis of bluetooth encryption with condition masking[C]//Advances in Cryptology-CRYPTO 2013. Berlin: Springer, 2013: 165-182.

[30] MEIER W, STAFFELBACH O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159-176.

[31] JOHANSSON T, JÖSSON F. Improved fast correlation attacks on stream ciphers via convolutional codes[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999: 347-362.

[32] JOHANSSON T, JÖNSSON F. Fast correlation attacks based on turbo code techniques[C]//Advances in Cryptology-CRYPTO'99. Berlin: Springer, 1999: 181-197.

[33] CANTEAUT A, TRABBIA M. Improved fast correlation attacks using parity-check equations of weight 4 and 5[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000: 573-588.

[34] GOLIC J D. Iterative optimum symbol-by-symbol decoding and fast correlation attacks[J]. IEEE Transactions on Information Theory, 2001, 47(7): 3040-3049.

[35] ZHOU Z C, FENG D, ZHANG B. Vectorial decoding algorithm for fast correlation attack and its applications to stream cipher grain-128a[J]. IACR Transactions on Symmetric Cryptology, 2022(2): 322-350.

[36] CHEPYZHOV V, JOHANSSON T, SMEETS B. A simple algorithm for fast correlation attacks on stream ciphers[C]//Fast Software Encryption 2000. Berlin: Springer, 2000: 181-195.

[37] JOHANSSON T, JÖSSON F. Fast correlation attacks through reconstruction of linear polynomials[C]//Annual International Cryptology Conference. Berlin: Springer, 2000: 300-315.

[38] MIHALJEVI M J, FOSSORIER M P C, IMAI H. Fast correlation attack algorithm with list decoding and an application[C]//Fast Software Encryption 2002. Berlin: Springer, 2002: 196-210.

[39] CHOSE P, JOUX A, MITTON M. Fast correlation attacks: an algorithmic point of view[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2002: 209-221.

[40] ZHANG B, XU C, MEIER W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0[C]//Advances in Cryptology-CRYPTO 2015. Berlin: Springer, 2015: 643-662.

[41] SHI Z, JIN C, ZHANG J, CUI T, et al. A correlation attack on full SNOW-V and SNOW-Vi[C]//Advances in Cryptology-EUROCRYPT 2022. Berlin: Springer, 2022:1-6.

[42] TODO Y, ISOBE T, MEIER W, et al. Fast correlation attack revisited[C]//Advances in Cryptology-CRYPTO 2018. Berlin: Springer, 2018: 129-159.

[43] WANG S C, LIU M C, LIN D D, et al. Fast correlation attacks on grain-like small state stream ciphers and cryptanalysis of plantlet Fruit-v2 and Fruit-80[R]. 2019.

[44] WATANABE D, BIRYUKOV A, CANNIÈRE C. A distinguishing attack of SNOW 2.0 with linear masking method[C]//Selected Areas in Cryptography. Berlin: Springer, 2004: 222-233.

[45] BIHAM E, et al. Differential cryptanalysis in stream ciphers[R]. 2007.

[46] ENGLUND H, JOHANSSON T, SÖNMEZ TURAN M. A framework for chosen IV statistical analysis of stream ciphers[C]//Lecture Notes in Computer Science. Berlin: Springer, 2007: 268-281.

[47] FISCHER S, KHAZAEI S, MEIER W. Chosen IV statistical analysis for key recovery attacks on stream ciphers[C]// Progress in Cryptology - AFRICACRYPT 2008. Berlin: Springer, 2008: 236-245.

[48] VIELHABER M. Breaking ONE.FIVIUM by AIDA an algebraic IV differential attack[R]. 2007.

[49] BIRYUKOV A, WAGNER D. Slide attacks[C]//Fast Software Encryption 1999. Berlin: Springer, 1999: 245-259.

[50] ZHANG B, LI Z Q, FENG D G, et al. Near collision attack on the grain v1 stream cipher[C]//Fast Software Encryption 2013. Berlin: Springer, 2014: 518-538.

[51] ZHANG B, XU C, MEIER W. Fast near collision attack on the grain v1 stream cipher[C]//EUROCRYPT 2018. Berlin: Springer, 2018: 771-802.

[52] DINUR I, SHAMIR A. Cube attacks on tweakable black box polynomials[C]//Advances in Cryptology - EUROCRYPT 2009. Berlin: Springer, 2009: 278-299.

[53] AUMASSON J, DINUR I, MEIER W, et al. Cube testers and key recovery attacks on reduced-round MD6 and trivium[C]//Fast Software Encryption 2009. Berlin: Springer, 2009: 1-22.

[54] AUMASSON P, DINUR I, HENZEN L, et al. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128[R]. 2009.

[55] DINUR I, SHAMIR A. Breaking Grain-128 with dynamic cube attacks[C]//Fast Software Encryption 2011. Berlin: Springer, 2011: 167-187.

[56] TODO Y, MORII M. Bit-based division property and application to Simon family[C]//Fast Software Encryption 2016. Berlin: Springer, 2016: 357-377.

[57] TODO Y, ISOBE T, HAO Y L, et al. Cube attacks on non-blackbox polynomials based on division property[C]//Advances in Cryptology - CRYPTO 2017. Berlin: Springer, 2017: 250-279.

[58] XIANG Z J, ZHANG W T, BAO Z Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers[C]//Advances in Cryptology-ASIACRYPT 2016. Berlin: Springer, 2016: 648-678.

[59] WANG Q J, HAO Y L, TODO Y, et al. Improved division property based cube attacks exploiting algebraic properties of superpoly[C]//Advances in Cryptology-CRYPTO 2018. Berlin: Springer, 2018: 275-305.

[60] WANG S P, HU B, GUAN J, et al. MILP-aided method of searching division property using three subsets and applications[C]//Advances in Cryptology -ASIACRYPT 2019. Berlin: Springer, 2019: 398-427.

[61] HAO Y L, LEANDER G, MEIER W, et al. Modeling for three-subset division property without unknown subset improved cube attacks against trivium and grain - 128AEAD[C]//EUEROCRYPT 2020. Berlin: Springer, 2020: 466-495.

[62] SUN Y. Automatic search of cubes for attacking stream ciphers[J]. IACR Transactions on Symmetric Cryptology, 2021(4): 100-123.

[63] HUANG S Y, WANG X Y, XU G W, et al. Conditional cube attacks on reduced-round Keccak sponge function[C]//EUROCRYPT 2017. Berlin: Springer, 2017: 259-288.

[64] WANG X Y, YU H B. How to break MD5 and other hash functions[C]//EUROCRYPT 2005. Berlin: Springer, 2005: 19-35.

[65] KNELLWOLF S, MEIER W, NAYA-PLASENCIA M. Conditional differential cryptanalysis of NLFSR-based cryptosystems[C]// Advances in Cryptology - ASIACRYPT 2010. Berlin: Springer, 2010: 130-145.

[66] LI Z, DONG X Y, WANG X Y. Conditional cube attack on round-reduced ASCON[J]. IACR Transactions on Symmetric Cryptology, 2017(1): 175-202.

[67] MULLER F. Differenctial attacks against the helix stream cipher[C]// Fast Software Encryption 2004. Berlin: Springer, 2004: 94-108.

[68] KÜÇÜK Ö. Slide resynchronization attack on the initialization of grain 1.0[R]. 2006.

[69] HAO Y L, JIAO L, LI C Y, et al. Links between division property and other cube attack variants[J]. IACR Transactions on Symmetric Cryptology, 2020(1): 363-395.

[70] KNUDSEN L, MEIER W, PRENEEL B, et al. Analysis methods for (alleged) RC4[C]//ASIACRYPT'98. Berlin: Springer, 1998: 327-341.

[71] PASALIC E. On guess and determine cryptanalysis of LFSR-based stream ciphers[J]. IEEE Transactions on Information Theory, 2009, 55(7): 3398-3406.

[72] FENG X T, LIU J, ZHOU Z C, et al. A byte-based guess and determine attack on SOSEMANUK[C]//ASIACRYPT 2010. Berlin: Springer, 2010: 146-157.

[73] YANG J, JOHANSSON T, MAXIMOV A. Improved guess-and-determine and distinguishing attacks on SNOW-V[J]. IACR Transactions on Symmetric Cryptology, 2021(3): 54-83.

[74] COURTOIS N T, MEIER W. Algebraic attacks on stream ciphers with linear feedback[C]//Eurocrypt 2003. Berlin: Springer, 2003: 345-359.

[75] ARS G, FAUGÈRE J C, IMAI H, et al. Comparison between XL and Gröbner basis algorithms[C]//Advances in Cryptology - ASIACRYPT 2004. Berlin: Springer, 2004: 338-353.

[76] COURTOIS N, KLIMOV A, PATARIN J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]//Advances in Cryptology EUROCRYPT 2000. Berlin: Springer, 2000: 392-407.

[77] COURTOIS N, PIEPRZYK J. Cryptanalysis of block ciphers with overdefined systems of equations[C]//Advances in Cryptology ASIACRYPT 2002. Berlin: Springer, 2002: 267-287.

[78] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]//Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 474-491.

[79] ARMKNECHT F. Improving fast algebraic attacks[C]//Fast Software Encryption 2004. Berlin: Springer, 2004: 65-82.

[80] BRAEKEN A, PRENEEL B. Probabilistic algebraic attacks[C]//Cryptography and Coding 2005. Berlin: Springer, 2005: 290-303.

[81] HAWKES P, ROSE G G. Rewriting variables: the complexity of fast correlation attacks on stream ciphers[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 390-406.

[82] HELLMAN M. A cryptanalytic time-memory trade-off[J]. IEEE Transactions on Information Theory, 1980, 26(4): 401-406.

[83] BIRYUKOV A, SHAMIR A. Cryptanalytic time/memory/data tradeoffs for stream ciphers[C]//Advances in Cryptology-ASIACRYPT 2000. Berlin: Springer, 2000: 1-13.

[84] BIRYUKOV A, SHAMIR A, WAGNER D. Real time cryptanalysis of A5/1 in a PC[C]// Fast Software Encryption 2000. Berlin: Springer, 2000: 1-18.

[85] MAITRA S, SINHA N, SIDDHANTI A, et al. A TMDTO attack against lizard[J]. IEEE Transactions on Computers, 2018, 67(5): 733-739.

[86] ESGIN M F, KARA O. Practical cryptanalysis of full sprout with TMD tradeoff attacks[C]//Selected Areas in Cryptography-SAC 2015. Berlin: Springer, 2015: 67-85.

[87] FUNABIKI Y, TODO Y, ISOBE T, et al. Several MILP-aided attacks against SNOW 2.0[C]//Cryptology and Network Security. Berlin: Springer, 2018: 394-413.

[88] CEN Z, FENG X T, WANG Z Y, et al. Minimizing deduction system and its application[J]. arXiv Preprint, arXiv: 2006.05833, 2020.

[89] BOURA C, COGGIA D. Efficient MILP modelings for sboxes and linear layers of SPN ciphers[J]. IACR Transactions on Symmetric Cryptology, 2020(3): 327-361.

[90] BEIERLE C, DERBEZ P, LEANDER G, et al. Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2[C]//Advances in Cryptology- EUROCRYPT 2021. Berlin: Springer, 2021: 155-183.

[91] SZMIDT J. The cube attack on courtois toy cipher[C]//Proceedings of International Conference on Number-Theoretic Methods in Cryptology. Berlin: Springer, 2017: 241-253.

[92] BEYNE T. A geometric approach to linear cryptanalysis[C]//ASIACRYPT 2021. Berlin: Springer, 2021: 36-66.

[93] 关杰, 丁林, 张凯. 序列密码的分析与设计[M]. 北京: 科学出版社, 2019.
GUAN J, DING L, ZHANG K. The cryptanalysis and design of stream ciphers[M]. Beijing: Science Press, 2019.

[94] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000.
FENG D G. The spectral theory and its applications in cryptology[M]. Beijing: Science Press, 2000.

[95] 冯登国. 密码分析学[M]. 北京: 清华大学出版社, 2000.
FENG D G. Cryptanalysis[M]. Beijing: Tsinghua University Press, 2000.

[作者简介]

周照存（1983− ），男，山东日照人，中国科学院软件研究所、中国科学院大学博士生，主要研究方向为流密码分析。

冯登国（1965− ），男，陕西靖边人，博士，中国科学院院士，中国科学院软件研究所研究员、博士生导师，主要研究方向为网络与信息安全。