**第一篇论文**

**论文题目：**Algebraic Meet-in-the-Middle Attack on LowMC

**作者：**Fukang Liu, Santanu Sarkar, Gaoli Wang, Willi Meier, Takanori Isobe

**历史背景与相关工作：**

LowMC是一种通用块密码家族，使用部分非线性层，是一种非常高效的置换置乱网络加密算法，基于矩阵的LFSR置换，对于128位密钥长度可以提供128位的安全性。但是，当密钥长度较小时，使用代数 Meet-in-the-Middle 攻击可以有效地降低破解难度。

该论文提到，过去对于使用部分非线性层的块密码家族的研究主要集中在在未经优化的情况下寻找差异和线性特性，许多方法都依赖于线性和差分特性，并不能针对非线性变换进行有效的攻击，过去集中于寻找差异或线性层的性质，但仍存在大量未被发掘的代数特性。在这种情况下，需要提出新的代数攻击技术，以发掘这些未被发掘的特性，达到最高的攻击效率。

**方法思想：**

该论文提出通过利用部分非线性层的特性来分析 LowMC，针对 LowMC 密码算法的部分非线性层特征进行了优化，降低了简单差分枚举攻击的内存复杂度，该攻击技术相对简单且可以降低比基于差分枚举的攻击技术更先进的内存复杂度。此外，该论文还提出了一种改进代数技术，用于从 LowMC 的差分路径中检索完整密钥，当差分路径中有足够多的活动S盒时，这种方法能将时间复杂度大大降低至常数级别。整个攻击的效率得到了进一步提高，并成功破解了一些LowMC实例。

**结论：**

在现有攻击方法的基础上，该论文提出的算法大大提高了密钥恢复的效率，并成功破解了一些LowMC实例，降低了LowMC和LowMC-M密码的安全保障，进一步突显了新原始设计的加密技术的重要性。该论文提出的攻击方法大幅降低了LowMC分组密码家族的安全性，证明了某些参数极易被破解。

**亮点：**

改论文通过分析S盒之间的联系，利用了部分非线性S盒的内部特征，恢复出完整密钥。这利用的是加密体制固有的漏洞，泛用性很强，效果也很好。

**不足之处：**

该论文提到的方法，在处理线性方程组时，当自由变量的数量增加时，由于难以限制其时间复杂度，因此解决这种非线性方程组的时间复杂度困难，而且在处理非活动S盒的方式相对低效，其时间复杂度仍然很高。

**第二篇论文**

**论文题目：**A Modular Approach to the Security Analysis of Two-Permutation Constructions

**作者：**Yu Long Chen

**历史背景与相关工作：**

随着轻量级原语的出现，对称加密中采用公共排列调用的构造变得越来越受欢迎，但是传统方法不适用于这些构造的安全性验证，而且过去的方法缺乏一种模块化的方法可以简化验证过程。所以该论文提出了一种分析这种基于公共排列的构造的安全性的方法。

**方法思想：**

该论文提出了一种基于模块化方法的新工具，可用于分析基于两个公共置换调用的构造的安全性，该工具建立在经典 mirror theory 的基础上，适用于理想置换模型下的安全证明。该论文提出了针对不同安全性概念适用的多个版本的公共置换 mirror theory，并提供了一个框架，可用于使用新技术的安全性分析。该论文提出的理论框架包括一个集合的坏事件，需要在安全分析中排除，但是当需要考虑非线性方程式时，安全分析变得非常复杂，可能会忽略一些坏事件。因此，在此框架中，我们需要将可能防止我们使用新技术的其他类型的组件排除在分析之外，防止发生此类情况。作者演示了将这个技术应用于Tweakable Even Mansour (TEM)、基于排列的Encrypted Davies-Mayer（pEDM）和基于排列的nonce-based Enhance Hash-then-Mask (nEHtMp)，证明了这些构造的多用户安全。

**结论：**

该论文针对基于两个独立置换调用的构造提出了一个新的理论，并提供了一种将该理论应用于构造的框架，以确定构造的解的数量下限，从而排除包含冲突的解。该论文提出的新理论可以适用于几乎所有流行的对称密钥加密安全模型，并提供了一组被认为是坏事件的相关概率需上限，需要在安全分析中予以考虑。在考虑到这些最坏事件的情况下，作者们的新理论得以应用于给定的系统，从而确定未知数的可能解的下限。

**不足之处：**

该论文提出的新理论可以适用于几乎所有流行的对称密钥加密安全模型，但是在现实生活中，广泛使用的密码模型是非对称加密模型，我认为这就是最大的不足，泛用性不强。