拓展的镜像理论及其在消息认证码中的应用

张 平, 秦佳琦

南京邮电大学 计算机学院、软件学院、网络空间安全学院 南京 中国 210023

摘要 拓展的镜像理论是一种用于界定含有仿射等式和不等式方程组系统中未知数的可能解数的方法论, 它在对称密码的可证明安全理论中发挥着重要的作用。论文再次聚焦拓展的镜像理论, 着力解决一个关键挑战: 为广泛参数范围内的仿射等式和不等式方程组系统中解数量建立鲁棒的下界估计。主要理论贡献体现在两大关键进展: 首先, 利用图论描述框架形式化地刻画了这些仿射系统固有的约束条件, 为分析提供了直观且强大的视角。其次, 基于这一图论视角, 为广泛参数范围内的此类系统建立了一个全新且显著改进的解数量下界, 为对称密码的普适抗生日界的严格证明奠定了理论基础。然后, 应用到两类重要消息认证码——基于两个伪随机置换并联构造的方案 EWCDMD 和基于两个伪随机置换级联构造的方案 EWCDM——的抗生日界安全性证明中, 展示了增强的拓展的镜像理论的实际效力。利用拓展的镜像理论框架和广泛参数下的鲁棒下界, 严格证明了 EWCDMD 和 EWCDM 均能达到抗生日界安全性。至关重要的是, 推导出了一个广泛范围内均适用的普适安全界, 证明了这两种构造均可提供 $2n/3$ 比特普适安全性, 其中 n 表示底层伪随机置换的比特长度。通过与以前的工作进行详细比较, 凸显了该工作的独特优势和崭新贡献。最后, 讨论了基于多个独立伪随机置换构造的抗生日界安全的消息认证码方案的安全性证明, 并遗留了基于多变量拓展的镜像理论的图理论完善的开放性问题。

关键词 拓展的镜像理论; 消息认证码; 图论; 伪随机置换; 抗生日界安全

中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2025.07.06

Extended Mirror Theory and Its Applications in Message Authentication Codes

ZHANG Ping, QIN Jiaqi

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Abstract The extended mirror theory is a methodology for bounding the possible number of solutions for affine systems of equalities and non-equalities with unknowns. It plays an important role in the provable security theory of symmetric ciphers. This paper focuses on the extended mirror theory again and addresses the critical challenge of establishing robust lower bounds for the solution count of affine systems of equalities and non-equalities across a wide parameter range. Our primary theoretical contribution manifests in two key advancements: First, we formalize the inherent constraints of these affine systems using a graph-theoretic description, offering an intuitive and powerful lens for analysis. Second, leveraging this graphical perspective, we establish a new and significantly improved lower bound on the number of solutions applicable to a wide parameter range of system configurations, which lays a theoretical foundation for the strict proof of the universal beyond the birthday bound (BBB) of symmetric ciphers. Then, the robust lower bounds for the solution count of such systems across a wide parameter range are applied to the BBB-security proof of two prominent Message Authentication Code (MAC) constructions: EWCDMD based on the parallel construction of two pseudo-random permutations and EWCDM based on the cascading construction of two pseudo-random permutations, demonstrating the practical power of our enhanced extended mirror theory. Utilizing the extended mirror theory framework and robust lower bounds under a wide parameter range, we rigorously prove that both EWCDMD and EWCDM achieve BBB security. Crucially, we derive a universal security bound valid across a wide operational range, demonstrating that both constructions offer up to $2n/3$-bit universal security, where n is the bit length of the underlying pseudo-random permutation. Detailed comparisons with prior works highlight the distinct advantages and novel contributions of our work. Finally, the BBB-secure MACs based on multiple independent pseudorandom permutations are discussed, and an open problem improving graph-theoretic refinements based on multivariable extended mirror theory is left.

Key words extended mirror theory; message authentication code; graph theory; pseudorandom permutation; beyond the birthday bound security

通讯作者: 张平, 博士研究生, 讲师, Email: zhgp@njupt.edu.cn。

本课题得到国家自然科学基金青年基金“可调认证加密方案设计与分析”(No. 61902195)资助。

收稿日期: 2023-06-04; 修改日期: 2023-09-07; 定稿日期: 2025-06-10

1 引言

镜像理论是 Patarin 首次提出并受多位密码学者青睐的数学方法, 它考虑一组以 $v \oplus y = \lambda$ 为形式的含有未知数的仿射等式方程组系统, 要求计算出满足该仿射等式方程组系统的未知数的可能解的数量的下界, 其中 v 和 y 是两个未知数, λ 是已知值[1-7]。镜像理论起初被命名为“$P_i \oplus P_j$ 定理”, 原因是其来源于 Bellare 等人[8]提出来“两个独立的分组密码的异或和是一个抗生日界安全的伪随机函数”, Patarin 首次使用镜像理论证明了这个结论并给出了抗生日界(实际上, 在此之前, Lucks[9]使用一个不同的方法也证明了这个结论, 并给出了相应的抗生日界)。镜像理论在抗生日界安全的伪随机函数的安全性分析中有着广泛应用[1-7,10-14]。但是对于抗生日界安全的消息认证码和认证加密方案的安全性分析中, 由于存在认证性(真实性、完整性、存在性不可伪造)安全指标, 单纯的使用镜像理论不足以进行安全性证明。因此, 考虑到未知数仿射等式方程组系统中可能也存在形如 $v \oplus y \neq \lambda$ 的仿射不等式方程组系统, Datta 等人提出了拓展的镜像理论[16-17]。拓展的镜像理论在抗生日界安全的消息认证码和认证加密方案的可证明安全理论中有着重要的应用[15-22]。

生日界瓶颈是大部分分组密码工作模式的共性问题, 即对于分组长度为 n 比特的工作模式, 其最多只能提供 $n/2$ 比特的安全性, 这个安全强度在一些特殊环境下是不够的。如 PRESENT 算法, 其分组长度是 64 比特, 被用于构造工作模式时, 安全性强度降为 32 比特, 这样的安全强度不足以保证工作模式的安全性。抗生日界安全就是安全性强度高于通常生日界。对于分组长度为 n 比特构造的抗生日界安全的工作模式方案, 能够提供超越 $n/2$ 比特的安全性。抗生日界安全的消息认证码方案可以用来确保信息的高度完整性(认证性、真实性、存在性不可伪造), 已有的设计方案数不胜数[16-26]。

1.1 主要的结果与贡献

论文聚焦拓展的镜像理论的通用图论描述, 从一个新的视角, 给出了拓展的镜像理论在图论描述形式下未知数解数的普适性下界, 然后将其应用于抗生日界安全的消息认证码的安全性证明中。具体来说, 论文的贡献包括:

首先, 考虑到2021年Datta等学者给出的拓展的镜像理论下界[17]在实际中参数 q_c 可能比较大的情况下无法确保要求的安全界问题, 即当 $q_c = O(2^{2n/3})$ 时, EWCDM 和 DWCDM 也只能确保 $2n/3$ 比特的安全性, 而且受到2023年Cogliati等人考虑广泛范围 ξ 下镜像理论研究的启发, 我们给出了针对广泛范围 q_c 下拓展的镜像理论的计数结果下界。

其次, 将拓展的镜像理论应用到基于独立伪随机置换并联和级联结构构造的抗生日界安全的消息认证码的可证明安全中, 给出了针对广泛范围 q_c 下的安全性证明, 并得到了普适性的安全界。

最后, 讨论了基于多个独立伪随机置换构造的抗生日界安全的消息认证码方案的安全性证明问题, 并遗留了基于多变量拓展的镜像理论的图理论完善的开放性问题。

1.2 相关工作

拓展的镜像理论是Datta等人[16]为证明消息认证码 DWCDM 的认证性安全而提出来的, 它是在 Patarin 的镜像理论基础上引入了仿射不等式方程组系统。2021 年, Datta 等学者[17]给出了匹配 EWCDM 和 DWCDM 方案的拓展的镜像理论描述, 从而改进了 EWCDM 和DWCDM的安全界, 实现了从 $2n/3$ 比特到 $3n/4$ 比特的安全性提升。后来, 拓展的镜像理论在抗生日界安全的消息认证码方案的可证明安全中被广泛使用[18-22]。2022 年, 陈玉龙教授[6]归纳总结提炼出了一种基于拓展的镜像理论的新工具, 用以模块化的方式分析了 TEM、pEDM 以及 nEHtMp 方案的多用户安全性。2023 年, Cogliati 等人[7]第一个给出了适用于大范围的 ξ 下镜像理论($P_i \oplus P_j$ 定理)的完整证明。采用链接删除方程技术, 有效的给出了该广泛范围下的镜像理论的抗生日界, 并将其应用到了两个最优安全的基于分组密码伪随机函数的安全证明以及六轮 Feistel 密码的安全证明中。同年, 包珍珍团队也将拓展的镜像理论应用到了新提出的抗生日界安全的认证加密工作模式XOCB的可证明安全中[15]。

2 基础知识

2.1 符号说明

论文中使用的一些基本符号描述如表 1 所示。

2.2 泛哈希函数(Universal 哈希函数)

泛哈希函数是一类具有特殊性质的哈希函数。给定一个哈希函数 $H: \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^n$, 对于任意两个输入 $x \neq x' \in \{0,1\}^*$ 和输出 $a \in \{0,1\}^n$, 都有

$$\Pr[K \leftarrow \{0,1\}^k : H(K,x) \oplus H(K,x') = a] \leqslant \varepsilon$$

则称 H 是 ε-almost XOR universal (AXU) 哈希函数。

如果 $\varepsilon = 2^{-n}$, 那么称此时 H 为 XU 哈希函数。

表 1 符号描述

Table 1 Symbols' descriptions

符号	含义
$\{0,1\}^n$	长度为 n 的比特串的集合
$\{0,1\}^*$	所有比特串的集合
$\|X\|$	集合 X 的元素个数或图 X 的顶点数
$X \oplus Y$	两个比特串 X 和 Y 的异或
$X\|\|Y$	两个比特串 X 和 Y 的连接
Perm(n)	$\{0,1\}^n$ 上所有置换的集合
Func(m,n)	从$\{0,1\}^m$到$\{0,1\}^n$的所有函数的集合
Func(n)	从$\{0,1\}^n$到$\{0,1\}^n$的所有函数的集合
$(2^n)_q$	$2^n(2^n-1)\cdots(2^n-q+1)$
$x \leftarrow X$	从集合 X 中随机选取一个 x
$\mathbf{A}^O=1$	事件: 对手 **A** 与预言机 O 交互之后输出 1
Pr[E]	事件 E 发生的概率

2.3 H 系数技术

H 系数技术是 Patarin 提出的一种用于区分真实密码方案与理想密码方案的概率优势上界方法[27]。假设 **A** 是一个确定性敌手, 可以查询真实密码方案 RE 和理想密码方案 ID, 并试图区分这两个方案。令脚本 $\tau = \{(x_1, y_1),...,(x_q, y_q)\}$ 表示 **A** 与方案 O (RE 或者 ID)经过 q 次交互得到的查询-应答对, 即对于所有的 i=1, …, q 都有 $O(x_i)=y_i$, 此时称 O 扩展脚本 τ, 记作 $O \triangleright \tau$。令 X_{re} 和 X_{id} 分别表示 **A** 与 RE 和 ID 交互之后脚本分布。如果 ID 的脚本概率分布大于 0, 即 $\Pr[X_{id} = \tau] > 0$, 就称这个脚本是可获得的。引入 H 系数技术引理如下:

引理 1 (H 系数技术[27]). 考虑所有可获得的脚本集合 Γ 的一个划分 $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$。如果存在 $\alpha \geqslant 0$ 使得

$$\Pr[X_{id} \in \Gamma_{bad}] \leqslant \alpha,$$

并且对于任意好的脚本 $\tau \in \Gamma_{good}$, 存在 $\beta \geqslant 0$, 都有

$$\frac{\Pr[X_{re} = \tau]}{\Pr[X_{id} = \tau]} \geqslant 1 - \beta,$$

则 **A** 攻击真实密码方案 RE 的优势为

$$\mathrm{Adv}(\mathbf{A}) = |\Pr[\mathbf{A}^{RE} = 1] - \Pr[\mathbf{A}^{ID} = 1]| \leqslant \alpha + \beta.$$

3 拓展的镜像理论

拓展的镜像理论是用来界定仿射等式和仿射不等式方程组中未知数解数的重要数学工具[16-17]。下面我们分别给出基于双变量拓展的镜像系统的方程描述、图论描述以及相应的约束条件和计数结果。

定义 1 (基于双变量拓展的镜像系统的方程描述) 给定整数 $q \geqslant 1$, $q_v \geqslant 1$ 和 $r \geqslant 1$。令 $X_1, \ldots, X_r$ 表示 r 个两两不同的 n 比特长的未知变量, $y_1, y_2, ..., y_{q+q_v}$ 表示 $q+q_v$ 个 n 比特长的常数(其中 $y_1, y_2, ..., y_q$ 对应等式方程组常数, 其余对应不等式方程组常数), 令

$$\varphi: \{a_1, b_1, ..., a_q, b_q\} \to \{1, 2, ..., r\}$$

$$\varphi': \{a_{q+1}, b_{q+1}, ..., a_{q+q_v}, b_{q+q_v}\} \to \{1, 2, ..., r\}$$

其中 φ 表示一个对应于仿射等式方程组系统的索引满射函数, φ' 表示一个对应于仿射不等式方程组系统的索引函数(不必是满射), 则拓展的镜像系统 S 可以描述为如下涵盖仿射等式方程组 $S^{=}$ 和不等式方程组 $S^{\neq}$ 的系统:

$$S^{=}: \begin{cases} X_{a_1} \oplus X_{b_1} = y_1 \\ X_{a_2} \oplus X_{b_2} = y_2 \\ \cdots\cdots \\ X_{a_q} \oplus X_{b_q} = y_q \end{cases} \quad S^{\neq}: \begin{cases} X_{a_{q+1}} \oplus X_{b_{q+1}} \neq y_{q+1} \\ X_{a_{q+2}} \oplus X_{b_{q+2}} \neq y_{q+2} \\ \cdots\cdots \\ X_{a_{q+q_v}} \oplus X_{b_{q+q_v}} \neq y_{q+q_v} \end{cases}$$

定义 2 (基于双变量拓展的镜像系统的图论描述) 如果将拓展的镜像系统中的随机变量看成是图的顶点, 每个仿射等式和不等式方程包含 2 个随机变量和一个常量, 把满足这个仿射方程的随机变量关系 (等式关系、不等式关系) 看作是图的边 (等边、不等边), 将满足这个仿射方程的常量看作是图中边的权。于是, 上面的镜像系统就可以看成是一个无向带权图, 记作 $G = <V, E, W>$。

- 顶点集: $V = V^{=} \cup V^{\neq} = \{X_1, ..., X_r\}$, 其中 $V^{=}$是仿射等式方程组系统的顶点集, 即由 $X_{a_1}, X_{b_1}, ..., X_{a_q}, X_{b_q}$ 不重复元素组成的顶点集, $V^{\neq}=V \setminus V^{=}$是仿射不等式方程组系统的顶点集。
- 边集: $E = E^{=} \cup E^{\neq} = \{\mathrm{e}_i = (X_{a_i}, X_{b_i})\}_{i=1}^{q+q_v}$, 其中 $E^{=} = \{e_1, ..., e_q\}$ 是仿射等式方程组系统的边集, 称为等边集; $E^{\neq} = \{e_{q+1}, ..., e_{q+q_v}\}$ 是仿射不等式方程组系统的边集, 称为不等边集。
- 权值函数: $W: E \to \{0,1\}^n$, 对于每一条边 $e_i \in E$, 都有 $W(e_i) = y_i$, 其中 $1 \leq i \leq q + q_v$。

拓展的镜像系统的约束条件。 为确保拓展的镜像系统的不重复性和一致性, 拓展的镜像系统图论形式下应满足如下的约束条件:

无圈性。 无向带权图 $G = <V, E, W>$ 的子图 $G^{=} = <V^{=}, E^{=}, W_{|E^{=}}>$ 里面, 其连通分支任意两顶点

之间只存在唯一的一条路径。

连通分支顶点数 ξ-最大。无向带权子图 $G^{=}=<V^{=},E^{=},W_{|E^{=}}>$ 的所有的连通分支中最大的连通分支的顶点数最多是 ξ。

非零路径权。定义路径 $Path$ 的权函数为这条路径上所有边的权值和, 即 $W(Path)=\sum_{e\in Path}W(e)=X_i\oplus X_j$, 其中 X_i 和 X_j 分别是该路径的起始点和终点。$G^{=}=<V^{=},E^{=},W_{|E^{=}}>$ 中不存在任何一条路径 $Path$ 使得 $W(Path)=0$。

非零圈权。定义一个圈 C 的权函数为这条圈上所有边的权值和, 即 $W(C)=\sum_{e\in C}W(e)$。在图 G 中不存在包含且仅包含一条不等边的圈 C 使得 $W(C)=0$。

无圈性, 说明拓展的镜像系统的方程组中通过线性组合一个或多个方程不会得到与随机变量 $X_1,\ldots,X_r$ 无关的方程。连通分支顶点数最大, 说明随机变量可以被划分为包含随机变量数最大的确定集合中, 即拓展的镜像系统的方程组中可以通过线性组合两个或多个方程得到含有随机变量最多的方程。非零路径权, 指的是拓展的镜像系统的方程组中通过线性组合一个或多个方程不会得到两个随机变量相等的方程。非零圈权, 反映的是拓展的镜像系统的方程组通过线性组合一个或多个方程不会得到关于两个随机变量关系相矛盾的两个方程。

假设 G 的子图 $G^{=}=<V^{=},E^{=},W_{|E^{=}}>$ 可以划分为 α 个顶点数大于等于 3 (边数大于等于 2) 的连通分支 $C_1\cup\cdots\cup C_\alpha$ 和 β 个顶点数恰好等于 2 (边数等于 1) 的连通分支 $D_1\cup\cdots\cup D_\beta$。令 $C=C_1\cup\cdots\cup C_\alpha$, $D=D_1\cup\cdots\cup D_\beta$, 则 $G^{=}=C\cup D$。定义 q_c 表示 α 个顶点数大于等于 3 的连通分支构成的子图 $C=C_1\cup\cdots\cup C_\alpha$ 的所有边数, 因此, 我们有 $q_c+\beta=q$ 并且 $2\alpha\leqslant q_c\leqslant q$。实际上, 在图 $G^{=}$ 中, 由于每个连通分支都是一个树, 因此, 每个连通分支的边数都是其顶点数减去 1。所以如果连通分支顶点数 ξ-最大, 则 $2\alpha\leqslant q_c\leqslant\alpha(\xi-1)$。此时, 我们发现 q_c 是有可能比较大的, 例如当 $q_c=O(2^{2n/3})$ 时, Datta 等学者[17]给出的拓展的镜像理论下界只能确保 $2n/3$ 比特的安全性, 此时是无法确保要求的 $3n/4$ 比特的安全性问题。因此, 这里我们考虑一个更广泛情况下的拓展的镜像理论的普适性安全性下界。与 Datta 等人工作[17]不同的是, 在已选好 C 的基础上选择补图 D 的所有可能计数, 这里我们没有再进一步细粒度化, 一方面是因为此时已有足够确保所需要的安全性界; 另一方面也是因为进一步细粒度化时, Datta 等人的两种特殊情况在 C 选好的情况下是不会发生的, 即对于从第 i 次选择 $D_1\cup\cdots\cup D_i$ 递推到第 $i+1$ 次选择 $D_1\cup\cdots\cup D_{i+1}$, 新增的两个顶点不能从前面选择, 否则就会与 α 个顶点数大于等于 3(边数大于等于 2)的连通分支相矛盾。于是, 我们有如下定理。

定理 1 (拓展的镜像理论的图论形式). 令 $G=<V,E,W>$ 是由拓展的镜像系统导出的无向带权图, 并且$|V|=r$, $|E|=q+q_v$。令 q_c 表示图中顶点数大于等于 3 的连通分支的总边数。则满足镜像系统的所有可能解的个数至少为

$$\frac{(2^n)_r}{2^{nq}}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{9q_c^2q+12q_cq^2+6q^3}{2^{2n}}-\frac{7q_v}{2^n}\right).$$

证明. 令 $h(G)$表示拓展的镜像系统 G 的解的个数。我们计算 $h(G)$的计数策略是: 先选择子图 $C=C_1\cup\cdots\cup C_\alpha$ (可能附带了部分不等式约束), 计算 C 的所有可能计数, 然后在已选好 C 的基础上选择子图 $D=D_1\cup\cdots\cup D_\beta$(可能附带了部分不等式约束), 计算 $C\cup D$ 的所有可能计数, 紧接着对不等式方程组系统图顶点(准确地说, 是对去掉与等式镜像系统相同顶点后的其他顶点)计数, 最后得到图 G 的所有可能计数。令 $h_c(i)$表示子图 $C_1\cup\cdots\cup C_i$ 的所有可能计数。令 $h_d(i)$表示子图 $C\cup D^i$ 的所有可能解计数, 这里 $C=C_1\cup\cdots\cup C_\alpha$ 已选定且 $D^i=D_1\cup\cdots\cup D_i$。令 $h_e(i)$表示 $V\setminus V^{=}$ 中前 i 个顶点的所有可能解计数, 这里 $V^{=}$已选定。

对于不等式方程组系统, 我们观察图 G 发现, 不等边只会来源于以下三种情况:

- 不等边的两个顶点都是来自顶点集 $V^{=}$, 且选自不同的连通分支。
- 不等边的两个顶点中有一个顶点来自顶点集 $V^{=}$。
- 不等边的两个顶点都不是来自顶点集 $V^{=}$。

假设 G 中的等式方程组系统第 i 个连通分支和第 j 个连通分支有 $\mu_{i,j}$ 条不等边, $V\setminus V^{=}$表示不在等式镜像系统顶点集中的不等式系统的顶点集, 假设其第 i 个顶点连接有 μ_i 条不等边。下面我们分别计算等式镜像系统中各连通分支的计数和不等式镜像系统中不在等式镜像系统的顶点计数。

我们先计算子图 $C=C_1\cup\cdots\cup C_\alpha$ 所有可能的解数 $h_c(\alpha)$ 的下界。假设 C_i 的顶点数是 w_i, 即 $w_i=|C_i|$, 并令 $\sigma_i=w_1+w_2+\cdots+w_i$, 其中 $1\leqslant i\leqslant\alpha$, 则有 $q_c=\sum_{i=1}^{\alpha}(w_i-1)=\sigma_\alpha-\alpha$。这里采用对每个连通分支的解进行计数的方式计算。首先, 对于第一个连通分支 C_1, 从连通分支中任选一个顶点进行赋值, 其

余顶点的值可通过等式连通关系唯一确定 (这适用于图中所有的连通分支)。由于顶点是从$\{0,1\}^n$集合中任意选取的, 所以有 2^n 种可能的选择。固定好第一个连通分支 C_1 的解之后, 我们考虑第二个连通分支 C_2 的所有可能的解数情况。同样地, 我们任取一个顶点, 要求这个顶点不能是第一个连通分支中的顶点, 而且, 一旦这个顶点选好之后, 由连通等式可以唯一确定其余顶点的值, 这些顶点也要求不能是第一个连通分支中的顶点。除此之外, 由于 C_2 和 C_1 两个连通分支之间存在了 $\mu_{2,1}$ 条不等边, 因此, C_2 中的顶点也不能取 $\mu_{2,1}$ 个违反不等边条件的值。所以, 考虑到赋值选择中存在的交叠情形, C_2 的所有可能的解总共至少有 $2^n-w_1-w_1(w_2-1)-\mu_{2,1}=2^n-w_1w_2-\mu_{2,1}$ 种选择。以此类推, 对于第 i 个连通分支 C_i, 一旦前 i-1 个连通分支的顶点被选好之后, 该连通分支的顶点赋值至少有 $2^n-\sigma_{i-1}w_i-\mu_{i,1}-\mu_{i,2}-\cdots-\mu_{i,i-1}$ 种选择。令 $\delta_i=\mu_{i,1}+\mu_{i,2}+\cdots+\mu_{i,i-1}$, $q_v^{'}=\sum_{i=1}^{\alpha}\delta_i$。于是, 对于 $C=C_1\cup\cdots\cup C_\alpha$, 所有可能的解数为

$$h_c(\alpha)\geqslant\prod_{i=1}^{\alpha}(2^n-\sigma_{i-1}w_i-\delta_i)\geqslant 2^{n\alpha}\left(1-\sum_{i=1}^{\alpha}\frac{\sigma_{i-1}w_i+\delta_i}{2^n}\right)$$

$$\geqslant 2^{n\alpha}\left(1-\frac{(\sum_{i=1}^{\alpha}w_i)^2}{2^n}-\sum_{i=1}^{\alpha}\frac{\delta_i}{2^n}\right)=2^{n\alpha}\left(1-\frac{\sigma_\alpha^2}{2^n}-\frac{q_v^{'}}{2^n}\right)$$

$$=2^{n\alpha}\left(1-\frac{(q_c+\alpha)^2}{2^n}-\frac{q_v^{'}}{2^n}\right)\geqslant 2^{n\alpha}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{q_v^{'}}{2^n}\right)$$

其中 $2\alpha\leqslant q_c\leqslant q$。

然后在已选好 C 的基础上选择补图 $D=D_1\cup\cdots\cup D_\beta$, 计算 $C\cup D^\beta$ 所有可能的解数 $h_d(\beta)$ 的下界, 其中 $C=C_1\cup\cdots\cup C_\alpha$ 并且 $D^\beta=D=D_1\cup\cdots\cup D_\beta$。与之前计算方法类似, 我们也只关注这 β 个单边的连通分支赋值, 采用对每个连通分支的解进行计数的方式计算。由于每个连通分支 D_i 的顶点数都是 2, 因此计数更加简单。类似于 $h_c(\alpha)$ 的计数过程, 对于第 $\alpha+i$ 个连通分支 D_i, 一旦前 $\alpha+i-1$ 个连通分支的顶点被选好之后, 该连通分支的顶点赋值至少有 $2^n-2(\sigma_\alpha+2(i-1))-\mu_{\alpha+i,1}-\mu_{\alpha+i,2}-\cdots-\mu_{\alpha+i,\alpha+i-1}$ 种选择。令 $\delta_{\alpha+i}=\mu_{\alpha+i,1}+\mu_{\alpha+i,2}\cdots+\mu_{\alpha+i,\ \alpha+i-1}$, $q_v^{''}=\sum_{i=1}^{\beta}\delta_{\alpha+i}$。于是, 在 C 已选好的基础上选择补图 $D=D_1\cup\cdots\cup D_\beta$, 计算 $C\cup D^\beta$ 所有可能的解数 $h_d(\beta)$ 为

$$h_d(\beta)\geqslant\prod_{i=1}^{\beta}(2^n-2\sigma_\alpha-4(i-1)-\delta_{\alpha+i})$$

紧接着, 我们对不在等式镜像系统中的不等式系统图顶点进行计数, 即考虑 $V\setminus V^{=}$。我们假设这样的不等顶点有 γ 个, 即 $\gamma=|V\setminus V^{=}|$。与之前计算方法类似, 但这里我们只关注这 γ 个顶点的赋值。对于第 i 个顶点, 一旦 $\alpha+\beta$ 个连通分支的 $\sigma_\alpha+2\beta$ 顶点和前 i-1 个顶点被选好之后, 考虑到第 i 个顶点连接 μ_i 条不等边, 则该顶点赋值至少有 $2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i$ 种选择。令 $q_v^{'''}=\sum_{i=1}^{\gamma}\mu_i$。于是, 在 $C\cup D$ 已选好的基础上选择其余的不等式系统的顶点, 计算 $V\setminus V^{=}$ 所有可能的解数 $h_e(\gamma)$ 为

$$h_e(\gamma)\geqslant\prod_{i=1}^{\gamma}(2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i)$$

从而, 进一步计算可得图 G 所有可能的解数 $h(G)$ 的下界:

$$h(G)\frac{2^{nq}}{(2^n)_r}\geqslant\underbrace{h_c(\alpha)\frac{2^{nq_c}}{(2^n)_{\sigma_\alpha}}}_{B.1}\cdot\underbrace{\frac{h_d(\beta)\cdot 2^{n\beta}}{(2^n-\sigma_\alpha)_{2\beta}}}_{B.2}\cdot\underbrace{\frac{h_e(\gamma)\cdot 2^0}{(2^n-\sigma_\alpha-2\beta)_\gamma}}_{B.3}$$

首先, **计算 B.1 的下界。** 由于 $q_c=\sigma_\alpha-\alpha$, 因此我们有

$$B.1=h_c(\alpha)\frac{2^{nq_c}}{(2^n)_{\sigma_\alpha}}\geqslant\frac{h_c(\alpha)}{2^{n\alpha}}\geqslant 1-\frac{9q_c^2}{4\cdot 2^n}-\frac{q_v^{'}}{2^n}$$

然后, **计算 B.2 的下界。**根据常用不等式: 对于任意 $0\leqslant a_1,...,a_k\leqslant 1$ 有 $\prod_{i=1}^{k}(1-a_i)\geqslant 1-\sum_{i=1}^{k}a_i$ 以及一些事实: $\sigma_\alpha+2i\leqslant q\leqslant 2^{n-1}$, $\beta\leqslant q$, $q_v^{''}=\sum_{i=1}^{\beta}\delta_{\alpha+i}$ 和 $\sigma_\alpha=q_c+\alpha$, 我们有

$$B.2=h_d(\beta)\frac{2^{n\beta}}{(2^n-\sigma_\alpha)_{2\beta}}$$

$$\geqslant\prod_{i=1}^{\beta}(2^n-2\sigma_\alpha-4(i-1)-\delta_{\alpha+i})\frac{2^{n\beta}}{(2^n-\sigma_\alpha)_{2\beta}}$$

$$=\prod_{i=1}^{\beta}\frac{(2^n-2\sigma_\alpha-4(i-1)-\delta_{\alpha+i})\cdot 2^n}{(2^n-\sigma_\alpha-2(i-1))_2}$$

$$\geqslant\prod_{i=1}^{\beta}\frac{(2^n-2\sigma_\alpha-4(i-1)-\delta_{\alpha+i})\cdot 2^n}{(2^n-\sigma_\alpha-2(i-1))^2}$$

$$=\prod_{i=1}^{\beta}\left(1-\frac{\sigma_\alpha^2+4(i-1)\sigma_\alpha+4(i-1)^2+\delta_{\alpha+i}\cdot 2^n}{(2^n-\sigma_\alpha-2(i-1))^2}\right)$$

$$\geqslant\prod_{i=1}^{\beta}\left(1-\frac{4\sigma_\alpha^2+16(i-1)\sigma_\alpha+16(i-1)^2+4\delta_{\alpha+i}\cdot 2^n}{2^{2n}}\right)$$

$$\geqslant 1-\sum_{i=1}^{\beta}\frac{4\sigma_\alpha^2+16(i-1)\sigma_\alpha+16(i-1)^2+4\delta_{\alpha+i}\cdot 2^n}{2^{2n}}$$

$$\geqslant 1-\frac{4\beta\sigma_\alpha^2+8\beta(\beta-1)\sigma_\alpha+3\beta(\beta-1)(2\beta-1)}{2^{2n}}-\frac{4q_v^{''}}{2^n}$$

$$\geqslant 1-\frac{9q_c^2q+12q_cq^2+6q^3}{2^{2n}}-\frac{4q_v^{''}}{2^n}$$

最后, **计算 B.3 的下界。**根据常用不等式: 对于任意 $0\leqslant a_1,...,a_k\leqslant 1$ 有 $\prod_{i=1}^{k}(1-a_i)\geqslant 1-\sum_{i=1}^{k}a_i$ 以及一些事实: $\sigma_\alpha+2\beta+i-1\leqslant 2^{n-1}$ 和 $q_v'''=\sum_{i=1}^{\gamma}\mu_i$, 我们有

$$
\begin{aligned}
B.3 &= h_e(\gamma)\frac{2^0}{(2^n-(\sigma_\alpha+2\beta))_\gamma}\\
&=\frac{\prod_{i=1}^{\gamma}(2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i)\cdot 2^0}{(2^n-(\sigma_\alpha+2\beta))_\gamma}\\
&=\prod_{i=1}^{\gamma}\frac{2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i}{2^n-(\sigma_\alpha+2\beta)-(i-1)}\\
&=\prod_{i=1}^{\gamma}\left(1-\frac{\mu_i}{2^n-(\sigma_\alpha+2\beta)-(i-1)}\right)\\
&\geqslant 1-\sum_{i=1}^{\gamma}\frac{\mu_i}{2^n-(\sigma_\alpha+2\beta)-(i-1)}\\
&\geqslant 1-\sum_{i=1}^{\gamma}\frac{2\mu_i}{2^n}=1-\frac{2q_v'''}{2^n}
\end{aligned}
$$

于是, 结合 B.1、B.2 和 B.3 的下界以及 $q_v'+q_v''+q_v'''=q_v$, 我们有

$$
h(G)\geqslant\frac{(2^n)_r}{2^{nq}}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{9q_c^2q+12q_cq^2+6q^3}{2^{2n}}-\frac{7q_v}{2^n}\right)
$$

定理 1 的结果得证。

对于上面的无向带权图 $G=<V,E,W>$ 进一步思考发现, 如果对于任意 $1\leqslant i\leqslant q+q_v$ 和 $1\leqslant j\leqslant q+q_v$ 都有 $X_{a_i}\neq X_{b_j}$, 则该图 $G=<V,E,W>$ 可以进一步描述为一个无向带权二部图 $G=<V_1,V_2,E,W>$, 其中 V_1 和 V_2 是 V 的二部划分, 即 $V_1\cup V_2=V, V_1\cap V_2=\varnothing$ 并且 V_1 是 $X_{a_1},...,X_{a_{q+q_v}}$ 构成的集合, V_2 是 $X_{b_1},...,X_{b_{q+q_v}}$ 构成的集合。此时, 拓展的镜像理论的二部图形式下得到的普适性安全下界如定理 2。

定理 2 (拓展的镜像理论的二部图形式). 令 $G=<V_1,V_2,E,W>$ 是由拓展的镜像系统导出的无向带权二部图, 并且 $|V_1|=q'$, $|V_2|=q''$, $|E|=q+q_v$。令 q_c 表示图中顶点数大于等于 3 的连通分支的总边数。则满足镜像系统的所有可能解的个数至少为

$$
\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{27q_c^2q+36q_cq^2+16q^3}{24\cdot 2^{2n}}-\frac{5q_v}{2^n}\right).
$$

证明. 定理 2 的证明与定理 1 的证明类似。令 $h(G)$ 表示拓展的镜像系统 G 的解的个数, $h_c(i)$ 表示子图 $C_1\cup\cdots\cup C_i$ 的所有可能计数, $h_d(i)$ 表示子图 $C\cup D^i$ 的所有可能解计数, 这里 $C=C_1\cup\cdots\cup C_\alpha$ 已选定且 $D^i=D_1\cup\cdots\cup D_i$。令 $h_e(i)$ 表示 $V\setminus V^=$ 中前 i 个顶点的所有可能解计数, 这里 $V^=$ 已选定。我们计算 $h(G)$ 的计数策略是: 先选择子图 $C=C_1\cup\cdots\cup C_\alpha$ (可能附带了部分不等式约束), 计算 C 的所有可能计数, 然后在已选好 C 的基础上选择子图 $D=D_1\cup\cdots\cup D_\beta$ (可能附带了部分不等式约束), 计算 $C\cup D$ 的所有可能计数, 紧接着对不等式方程组系统图顶点(准确地说, 是对去掉与等式镜像系统相同顶点后的其他顶点) 计数, 最后得到图 G 的所有可能计数。

我们先计算子图 $C=C_1\cup\cdots\cup C_\alpha$ 所有可能的解数 $h_c(\alpha)$ 的下界。假设 C_i 的顶点集是 V_{C_i}, 我们将其划分为左顶点集 $V_{1,i}=V_1\cap V_{C_i}$ 和右顶点集 $V_{2,i}=V_2\cap V_{C_i}$, 并令 $v_{1,i}=|V_{1,i}|$, $v_{2,i}=|V_{2,i}|$。对于 $1\leqslant i\leqslant\alpha$, 令 $\sigma_i=(v_{1,1}+v_{2,1})+...+(v_{1,i}+v_{2,i})$, 则有 $q_c=\sum_{i=1}^{\alpha}(v_{1,i}+v_{2,i}-1)=\sigma_\alpha-\alpha$。这里采用对每个连通分支的顶点进行计数的方式计算。首先, 对于第一个连通分支 C_1, 从连通分支中任选一个顶点进行赋值 (不妨假设我们都是从左顶点集中任选一个顶点), 其余顶点的值可通过等式连通关系唯一确定 (这适用于图中所有的连通分支的左右顶点)。由于顶点是从 $\{0,1\}^n$ 集合中任意选取的, 所以有 2^n 种可能的选择。固定好第一个连通分支 C_1 的解之后, 我们考虑第二个连通分支 C_2 的所有可能的解数情况。同样地, 我们从左顶点集 $V_{1,2}$ 中任取一个顶点, 要求这个顶点不能是第一个连通分支中的左顶点, 而且, 一旦这个顶点选好之后, 由连通等式可以唯一确定其余顶点的值, 并且这些其余顶点中落在 C_2 左顶点集 $V_{1,2}$ 的顶点也要求不能是第一个连通分支中的左顶点, 落在 C_2 右顶点集 $V_{2,2}$ 的顶点也要求不能是第一个连通分支中的右顶点。除此之外, 由于 C_2 和 C_1 两个连通分支之间存在了 $\mu_{2,1}$ 条不等边, 因此, C_2 中的顶点也不能取 $\mu_{2,1}$ 个违反不等边条件的值。因此, 考虑到赋值选择中存在的交叠情形, C_2 的所有可能的解总共至少有 $2^n-v_{1,1}v_{1,2}-v_{2,1}v_{2,2}-\mu_{2,1}$ 种选择。以此类推, 对于第 i 个连通分支 C_i, 一旦前 i-1 个连通分支的顶点被选好之后, 该连通分支的顶点赋值至少有 $2^n-(v_{1,1}+\cdots+v_{1,i-1})v_{1,i}-(v_{2,1}+\cdots+v_{2,i-1})v_{2,i}-\mu_{i,1}-\mu_{i,2}-\cdots-\mu_{i,i-1}$ 种选择。令 $\delta_i=\mu_{i,1}+\mu_{i,2}+\cdots+\mu_{i,i-1}$, $q_v'=\sum_{i=1}^{\alpha}\delta_i$。于是, 对于 $C=C_1\cup\cdots\cup C_\alpha$, 所有可能的解数为

$$h_c(\alpha)\geqslant\prod_{i=1}^{\alpha}(2^n-(v_{1,1}+\ldots+v_{1,i-1})v_{1,i}-(v_{2,1}+\ldots+v_{2,i-1})v_{2,i}-\delta_i)$$
$$\geqslant 2^{n\alpha}\left(1-\sum_{i=1}^{\alpha}\frac{(v_{1,1}+\ldots+v_{1,i-1})v_{1,i}+(v_{2,1}+\ldots+v_{2,i-1})v_{2,i}+\delta_i}{2^n}\right)$$
$$=2^{n\alpha}\left(1-\sum_{i=1}^{\alpha}\sum_{j=1}^{i-1}\frac{v_{1,j}v_{1,i}+v_{2,j}v_{2,i}}{2^n}-\sum_{i=1}^{\alpha}\frac{\delta_i}{2^n}\right)$$
$$\geqslant 2^{n\alpha}\left(1-\frac{(\sum_{i=1}^{\alpha}v_{1,i}+v_{2,i})^2}{2^n}-\frac{q_v^{'}}{2^n}\right)=2^{n\alpha}\left(1-\frac{\sigma_\alpha^2}{2^n}-\frac{q_v^{'}}{2^n}\right)$$
$$=2^{n\alpha}\left(1-\frac{(q_c+\alpha)^2}{2^n}-\frac{q_v^{'}}{2^n}\right)\geqslant 2^{n\alpha}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{q_v^{'}}{2^n}\right)$$

然后在已选好 C 的基础上选择补图 $D=D_1\cup\cdots\cup D_\beta$, 计算 $C\cup D^\beta$ 所有可能的解数 $h_d(\beta)$ 的下界, 其中 $C=C_1\cup\cdots\cup C_\alpha$ 并且 $D^\beta=D=D_1\cup\cdots\cup D_\beta$。与之前计算方法类似, 我们也只关注这 β 个单边的连通分支赋值, 采用对每个连通分支的解进行计数的方式计算。由于每个连通分支 D_i 的顶点数都是 2 (左顶点数和右顶点数都为 1), 因此计数更加简单。令 $v_1=v_{1,1}+v_{1,2}+\cdots+v_{1,\alpha}$ 和 $v_2=v_{2,1}+v_{2,2}+\cdots+v_{2,\alpha}$, 则有 $v_1+v_2=\sigma_\alpha$。类似于 $h_c(\alpha)$ 的计数过程, 对于第 $\alpha+i$ 个连通分支 D_i, 一旦前 $\alpha+i-1$ 个连通分支的顶点被选好之后, 该连通分支的顶点赋值至少有 $2^n-v_1-(i-1)-v_2-(i-1)-\delta_{\alpha+i}=2^n-\sigma_\alpha-2(i-1)-\delta_{\alpha+i}$ 种选择, 其中 $\delta_{\alpha+i}=\mu_{\alpha+i,1}+\mu_{\alpha+i,2}\cdots+\mu_{\alpha+i,\alpha+i-1}$。令 $q_v^{''}=\sum_{i=1}^{\beta}\delta_{\alpha+i}$。于是, 在 C 已选好的基础上选择补图 $D=D_1\cup\cdots\cup D_\beta$, 计算 $C\cup D^\beta$ 所有可能的解数 $h_d(\beta)$ 为

$$h_d(\beta)\geqslant\prod_{i=1}^{\beta}(2^n-\sigma_\alpha-2(i-1)-\delta_{\alpha+i})$$

紧接着, 我们对不在等式镜像系统中的不等式系统图顶点进行计数, 即考虑 $V\setminus V^{=}$。我们假设这样的不等顶点有 γ 个, 即 $\gamma=|V\setminus V^{=}|$。与之前计算方法类似, 但这里我们只关注这 γ 个顶点的赋值。对于第 i 个顶点, 一旦 $\alpha+\beta$ 个连通分支的 $\sigma_\alpha+2\beta$ 顶点和前 i-1 个顶点被选好之后, 考虑到第 i 个顶点连接 μ_i 条不等边, 则该顶点赋值至少有 $2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i$ 种选择。令 $q_v^{'''}=\sum_{i=1}^{\gamma}\mu_i$。于是, 在 $C\cup D$ 已选好的基础上选择其余的不等式系统的顶点, 计算 $V\setminus V^{=}$ 所有可能的解数 $h_e(\gamma)$ 为

$$h_e(\gamma)\geqslant\prod_{i=1}^{\gamma}(2^n-(\sigma_\alpha+2\beta)-(i-1)-\mu_i)$$

从而, 进一步计算可得图 G 所有可能的解数 $h(G)$的下界:

$$h(G)\frac{2^{nq}}{(2^n)_{q'}(2^n)_{q''}}\geqslant\underbrace{h_c(\alpha)\frac{2^{nq_c}}{(2^n)_{v_1}(2^n)_{v2}}}_{B.1}$$
$$\cdot\underbrace{h_d(\beta)\frac{2^{n\beta}}{(2^n-v_1)_\beta(2^n-v_2)_\beta}}_{B.2}\cdot\underbrace{h_e(\gamma)\frac{2^0}{(2^n-\sigma_\alpha-2\beta)_\gamma}}_{B.3}$$

根据定理 1, 我们有 B.1 和 B.3 的下界:

$$B.1=h_c(\alpha)\frac{2^{nq_c}}{(2^n)_{\sigma_\alpha}}\geqslant\frac{h_c(\alpha)}{2^{n\alpha}}\geqslant 1-\frac{9q_c^2}{4\cdot 2^n}-\frac{q_v^{'}}{2^n}$$

$$B.3=h_e(\gamma)\frac{2^0}{(2^n-(\sigma_\alpha+2\beta))_\gamma}\geqslant 1-\frac{2q_v^{'''}}{2^n}$$

然后, **计算 B.2 的下界。**根据常用不等式: 对于任意 $0\leqslant a_1,\ldots,a_k\leqslant 1$ 有 $\prod_{i=1}^{k}(1-a_i)\geqslant 1-\sum_{i=1}^{k}a_i$ 以及一些事实: $\sigma_\alpha+2i\leqslant q\leqslant 2^{n-1}$, $\beta\leqslant q$, $q_v^{''}=\sum_{i=1}^{\beta}\delta_{\alpha+i}$ 和 $v_1+v_2=\sigma_\alpha=q_c+\alpha$, 我们有

$$B.2=h_d(\beta)\frac{2^{n\beta}}{(2^n-v_1)_\beta(2^n-v_2)_\beta}$$
$$\geqslant\prod_{i=1}^{\beta}\frac{(2^n-\sigma_\alpha-2(i-1)-\delta_{\alpha+i})2^{n\beta}}{(2^n-v_1)_\beta(2^n-v_2)_\beta}$$
$$=\prod_{i=1}^{\beta}\frac{(2^n-\sigma_\alpha-2(i-1)-\delta_{\alpha+i})\cdot 2^n}{(2^n-v_1-(i-1))(2^n-v_2-(i-1))}$$
$$=\prod_{i=1}^{\beta}\left(1-\frac{v_1v_2+(i-1)\sigma_\alpha+(i-1)^2+\delta_{\alpha+i}\cdot 2^n}{(2^n-v_1-(i-1))(2^n-v_2-(i-1))}\right)$$
$$\geqslant 1-\sum_{i=1}^{\beta}\frac{v_1v_2+(i-1)\sigma_\alpha+(i-1)^2+\delta_{\alpha+i}\cdot 2^n}{(2^n-v_1-(i-1))(2^n-v_2-(i-1))}$$
$$\geqslant 1-\frac{6\beta\sigma_\alpha^2+12\beta(\beta-1)\sigma_\alpha+4\beta(\beta-1)(2\beta-1)}{24\cdot 2^{2n-1}}-\frac{q_v^{''}}{2^{n-1}}$$
$$\geqslant 1-\frac{27q_c^2q+36q_cq^2+16q^3}{24\cdot 2^{2n}}-\frac{2q_v^{''}}{2^n}$$

于是, 结合 B.1、B.2 和 B.3 的下界以及 $q_v^{'}+q_v^{''}+q_v^{'''}=q_v$, 我们有

$$h(G)\geqslant \frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q_c^2}{4\cdot 2^n}-\frac{27q_c^2q+36q_cq^2+16q^3}{24\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)$$

定理 2 的结果得证。

4 应用到消息认证码

基于 nonce 的消息认证码(MAC)[28]通常可以处理任意长度的消息, 并生成认证标签, 它包括以下 3 个算法:

(1) 密钥生成算法 *KeyGen*: 是一个随机算法, 用于生成双方所共有的密钥 K;

(2) MAC 生成算法 *MAC*: 以密钥 K、状态 nonce N 和消息 M 为输入, 输出标签 T;

(3) 验证算法 *VF*: 是一个确定性算法, 以密钥 K、状态 nonce N、消息 M 和标签 T 为输入, 输出 1 比特决策值。对于验证算法 *VF*, 考虑如下形式, 即输入密钥 K、状态 nonce N、消息 M 给 *MAC* 算法, 计算得出的标签与标签 T 进行比较, 如果不相等, 则验证失败, 返回 0; 如果相等, 则验证成功, 返回 1。

敌手攻击 MAC 的具体过程如下:

首先, 在学习阶段, 敌手通过查询 *MAC* 算法可以获得他想知道的任何状态消息的认证标签。具体来说, 假设敌手做 q 次 *MAC* 查询 $(N_1, M_1),\cdots,(N_q, M_q)$, 生成标签 $T_1,\cdots, T_q$, 即对应如下一个仿射等式方程组系统:

$$\begin{aligned}&MAC_K(N_1,M_1)=T_1,\\&MAC_K(N_2,M_2)=T_2,\\&.....\\&MAC_K(N_q,M_q)=T_q.\end{aligned}$$

然后, 对手进入伪造阶段, 对手伪造新的状态消息-标签对, 如果能够通过验证算法 *VF* 验证成功而且该状态消息从未被查询过, 那么就称敌手伪造攻击成功了, 输出 1, 否则输出 0。具体来说, 假设对手做 q_v 次伪造查询 $(N_1^{'},M_1^{'},T_1^{'}),\cdots,(N_{q_v}^{'},M_{q_v}^{'},T_{q_v}^{'})$, 其中状态消息 $(N_1^{'},M_1^{'}),...,(N_{q_v}^{'},M_{q_v}^{'})$ 从未被查询过, 如果所有的伪造查询都没有通过验证预言机, 则称敌手伪造失败了, 返回 0, 即对应如下一个仿射不等式方程组系统:

$$\begin{aligned}&MAC_K(N_1^{'},M_1^{'})\neq T_1^{'},\\&MAC_K(N_2^{'},M_2^{'})\neq T_2^{'},\\&.....\\&MAC_K(N_{q_v}^{'},M_{q_v}^{'})\neq T_{q_v}^{'}.\end{aligned}$$

对于敌手 **A**, 用伪造优势来定义敌手 **A** 伪造攻击成功的概率, 它反映了敌手的攻击能力, 如果对最聪明的攻击者, 在一定的资源下, 伪造优势充分小, 我们就称该消息认证码是 MAC 安全的, 下面给出 MAC 安全性定义。

定义 3 (MAC 安全). 令 $\Pi=(KeyGen,MAC,VF)$ 是一个基于 nonce 的消息认证码, 定义对手 **A** 的 MAC 安全优势为:

$$Adv_{\Pi}^{\mathrm{mac}}(\mathbf{A})=Pr[K\leftarrow KeyGen:\mathbf{A}^{MAC_K,VF_K}\ forges]$$

进一步地, 为了方便使用 H 系数技术。我们将 MAC 安全优势使用不可区分优势的形式定义, 得到 MAC 优势的上界。令\$是 *MAC* 的理想版本, 即给定任意输入, 输出总是从均匀随机分布中任选的。$\perp$ 表示拒绝预言机, 即对于任意输入, 输出总是 0。则对手 **A** 的 MAC 优势的上界为:

$$Adv_{\Pi}^{\mathrm{mac}}(\mathbf{A})\leqslant|Pr[\mathbf{A}^{MAC_K,VF_K}=1]-Pr[\mathbf{A}^{\$,\perp}=1]|$$

消息认证码的设计一直是密码学者关注的重点问题, 其设计方法、设计思路以及设计方案层出不穷。下面我们主要介绍并级联模型设计的两种典型抗生日界安全的消息认证码方案 EWCDMD 和 EWCDM, 以及拓展的镜像理论在其证明过程中的使用。

4.1 应用到并联结构的 EWCDMD 方案

令 P_1, P_2 是两个独立的 n 比特长的伪随机置换, N 是一个 nonce-respecting 的 nonce(即要求加密使用的 nonce 都不同), H 是一个 ϵ-AXU 哈希函数, 则从任意比特长的消息 M 到 n 比特长的标签 T 的基于 nonce 的消息认证码 EWCDMD 方案如下:

$$T=P_2(P_1(N)\oplus H(M))\oplus P_1(N)\oplus H(M)$$

定理 3. 假设对手 **A** 做 q 次 *MAC* 查询和 q_v 次伪造尝试, 则 EWCDMD 方案的 MAC 安全优势为:

$$Adv_{EWCDMD}^{\mathrm{mac}}(\mathbf{A})\leqslant\frac{13.5q+q^2\varepsilon+5q^{3/2}+5q_v}{2^n}.$$

证明. 定理3的证明使用H系数技术和拓展的镜像理论。令\$是 *MAC* 算法的理想版本, 总是返回一个与输出等长的随机比特串。令 $\perp$ 表示拒绝预言机(*VF* 算法的理想版本), 即对于任意输入, 输出总是 0。假设 **A** 是一个确定性对手, 它能查询真实构造方案 *(MAC, VF)*, 也能查询真实构造方案的理想方案 (\$, $\perp$), 并将其与它们的交互过程记作 $\mathbf{A}^{MAC,VF}$ 或者 $\mathbf{A}^{\$,\perp}$。假设敌手 **A** 做 q 次 *MAC* 查询和 q_v 次伪造尝试 (*VF* 查询), 我们将敌手与 *MAC* 预言机和 *VF* 预言机交互之后的查询应答对记作脚本 $\tau=\{(N_1,M_1,T_1),...,(N_q,M_q,T_q),(N_1^{'},M_1^{'},T_1^{'}),...,(N_{q_v}^{'},$

$M_{q_v}^{'},T_{q_v}^{'})\}$。根据 nonce-respecting 的特点, 敌手查询 *MAC* 预言机 nonce 值都不同, 即对于 $1\leqslant i\neq j\leqslant q$ 都有 $N_i\neq N_j$。

根据敌手交互查询得到的应答脚本 $\tau=\{(N_1,M_1,T_1),...,(N_q,M_q,T_q),(N_1^{'},M_1^{'},T_1^{'}),...,(N_{q_v}^{'},M_{q_v}^{'},T_{q_v}^{'})\}\neq$, 定义如下包含 q 个仿射等式方程组系统和 q_v 个不等式方程组系统组成的拓展的镜像系统 *S*:

$$S^{=}:\begin{cases}P_2(P_1(N_1)\oplus H(M_1))\oplus P_1(N_1)=T_1\oplus H(M_1)\\ P_2(P_1(N_2)\oplus H(M_2))\oplus P_1(N_2)=T_2\oplus H(M_2)\\ \quad\cdots\cdots\\ P_2(P_1(N_q)\oplus H(M_q))\oplus P_1(N_q)=T_q\oplus H(M_q)\end{cases}$$

$$S^{\neq}:\begin{cases}P_2(P_1(N_1^{'})\oplus H(M_1^{'}))\oplus P_1(N_1^{'})\neq T_1^{'}\oplus H(M_1^{'})\\ P_2(P_1(N_2^{'})\oplus H(M_2^{'}))\oplus P_1(N_2^{'})\neq T_2^{'}\oplus H(M_2^{'})\\ \quad\cdots\cdots\\ P_2(P_1(N_{q_v}^{'})\oplus H(M_{q_v}^{'}))\oplus P_1(N_{q_v}^{'})\neq T_{q_v}^{'}\oplus H(M_{q_v}^{'})\end{cases}$$

令 $X_{a_i}=P_2(P_1(N_i)\oplus H(M_i))$, $X_{b_i}=P_1(N_i)$, $y_i=T_i\oplus H(M_i)$, 由于 $N_i\neq N_j$, 因此, $X_{b_i}\neq X_{b_j}$, 这里 $1\leqslant i\neq j\leqslant q$。令 $X_{a_{q+i}}=P_2(P_1(N_i^{'})\oplus H(M_i^{'}))$, $X_{b_{q+i}}=P_1(N_i^{'})$, $y_{q+i}=T_i^{'}\oplus H(M_i^{'})$, 这里 $1\leqslant i\leqslant q_v$。由于 P_1, P_2 都是随机选取的, 因此, $X_{a_i}\neq X_{b_j}$, 这里 $1\leqslant i\neq j\leqslant q+q_v$。则上面拓展的镜像系统可以描述为一个无向带权二部图 $G=<V_1,V_2,E,W>$, 其中

- V_1 是由 $X_{a_1},...,X_{a_{q+q_v}}$ 不重复元素组成的顶点集, V_2 是由集合 $\{X_{b_1},...,X_{b_q}\}$ 和 $X_{b_{q+1}},...,X_{b_{q+q_v}}$ 不重复元素组成的顶点集, 并且 $V_1^{=}$是由 $X_{a_1},...,X_{a_q}$ 不重复元素组成的仿射等式方程组系统的顶点集, $V_2^{=}=\{X_{b_1},...,X_{b_q}\}$。
- $E=E^{=}\cup E^{\neq}=\{e_i=(X_{a_i},X_{b_i})\}_{i=1}^{q+q_v}$, 其中 $E^{=}=\{e_1,...,e_q\}$ 是仿射等式方程组系统的等边集; $E^{\neq}=\{e_{q+1},...,e_{q+q_v}\}$ 是仿射不等式方程组系统的不等边集。
- $W:E\to\{0,1\}^n$, 对于每一条边 $e_i\in E$, 都有 $W(e_i)=y_i$, 其中 $1\leqslant i\leqslant q+q_v$。

在真实方案中, 对于任意的 $1\leqslant i\neq j\leqslant q$, 如果存在 $P_2(P_1(N_i)\oplus H(M_i))=P_2(P_1(N_j)\oplus H(M_j))$, 即 $X_{a_i}=X_{a_j}$, 则称存在一个碰撞的脚本事件。假设存在 $P_2(P_1(N_i)\oplus H(M_i))=P_2(P_1(N_j)\oplus H(M_j))$, 则有

$$P_1(N_i)\oplus H(M_i)=P_1(N_j)\oplus H(M_j)$$
$$\Leftrightarrow P_1(N_i)\oplus P_1(N_j)=H(M_i)\oplus H(M_j)$$

根据仿射等式方程组系统, 也有

$$P_2(P_1(N_i)\oplus H(M_i))=P_2(P_1(N_j)\oplus H(M_j))$$
$$\Leftrightarrow P_1(N_i)\oplus P_1(N_j)=T_i\oplus H(M_i)\oplus T_j\oplus H(M_j)$$

于是, 得到 $T_i=T_j$。这说明 $X_{a_i}=X_{a_j}\Leftrightarrow T_i=T_j$。除此之外, 对于任意的 $1\leqslant i\neq j\leqslant q$, 如果 $T_i=T_j$ 并且 $H(M_i)=H(M_j)$, 则与 $N_i\neq N_j$ 相矛盾。考虑到拓展的镜像系统的约束条件情况, 我们先定义一个“坏” 的脚本记录。

定义 4 (“坏”的脚本记录). 对于一个脚本记录 τ, 如果 $|T_i=T_j|>\sqrt{q}$ 或者 $T_i=T_j$ 并且 $H(M_i)=H(M_j)$, 其中 $1\leqslant i\neq j\leqslant q$, 那么我们称 τ 是 “坏” 的。

令 Γ 表示所有可获得的脚本记录集合, Γ_{bad} 表示所有 “坏”的脚本记录集合, $\Gamma_{good}=\Gamma\setminus\Gamma_{bad}$。下面, 根据 H 系数技术 (引理 1), 给出理想方案中 “坏”的脚本记录发生的概率。

在理想方案中, 根据马尔科夫不等式 $\Pr[X\geqslant a]\leqslant\frac{E(X)}{a}$ 和 ϵ-AXU 哈希函数的定义, 有

$$\begin{aligned}&\Pr[X_{id}\in\Gamma_{bad}]\\&=\Pr[|T_i=T_j|\geqslant\sqrt{q}]+\Pr[T_i=T_j,H(M_i)=H(M_j)]\\&\leqslant\frac{E[|T_i=T_j|]}{\sqrt{q}}+\frac{q^2\varepsilon}{2^n}\leqslant\frac{q^{3/2}}{2^n}+\frac{q^2\varepsilon}{2^n}\end{aligned}$$

在“好”的脚本记录下, 拓展的镜像系统满足约束条件:

无圈性。由于对于任意的 $1\leqslant i,j\leqslant q$ 都有 $X_{a_i}\neq X_{b_j}$, 因此, 无向带权图中任意两顶点之间至多只存在一条路径。

连通分支顶点数 ($2\sqrt{q}-1$) 最大。根据 $|T_i=T_j|\leqslant\sqrt{q}-1$ 即 $|X_{a_i}=X_{a_j}|\leqslant\sqrt{q}-1$, 也就是集合 V_1 中相等的顶点数最多为$\sqrt{q}-1$。因此, 子图 $G^{=}$ 中顶点数大于 2 的所有连通分支的总边数至多为 $2(\sqrt{q}-1)$。结合子图 $G^{=}$的等式连通关系 (连通分支), 可以将顶点集 V 划分为若干个非空子集。根据连通分支是树的性质, 子图$G^{=}$中连通分支顶点数最多等于 $2\sqrt{q}-1$。

非零路径权。对于任意的 $1\leqslant i,j\leqslant q$ 都有 $X_{a_i}\neq X_{b_j}$, $X_{b_i}\neq X_{b_j}$, 所以子图 $G^{=}$中不存在任何一

条路径 $Path$ 使得 $W(Path)=0$。

非零圈权。由于对于任意的 $1\leqslant i, j\leqslant q$ 都有 $X_{a_i}\neq X_{b_j}$, $X_{b_i}\neq X_{b_j}$, 所以图 G 中不存在包含且仅包含一条不等边的圈 C 使得 $W(C)=0$。

假设拓展的镜像系统中 $|V_1|=q'$, $|V_2|=q''$, 因此, 根据拓展的镜像理论的二部图描述定理 2, 真实方案导出的镜像系统解的个数至少是

$$\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)$$

于是, 真实方案在“好”的脚本 τ 下, 除这 r 个随机变量$\{X_1,\cdots, X_r\}$之外的值, 是按照独立随机置换来取值。因此有

$$\begin{aligned}\Pr[X_{re}=\tau]&=\Pr[P_1,P_2\leftarrow Perm(n): EWCDMD\triangleright\tau]\\&\geqslant\frac{\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)\cdot(2^n-q')!(2^n-q'')!}{(2^n!)^2}\\&\geqslant\frac{1}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)\end{aligned}$$

而理想方案在 “好”的脚本 τ 下, 都是随机选取的, 因此有

$$\Pr[X_{id}=\tau]=\frac{1}{2^{nq}}$$

于是, 对于所有“好”的脚本 τ, 我们有

$$\frac{\Pr[X_{re}=\tau]}{\Pr[X_{id}=\tau]}\geqslant 1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}.$$

根据 H 系数技术引理 (引理 1), 有

$$\begin{aligned}Adv^{mac}_{EWCDMD}(\mathbf{A})&\leqslant\frac{q^{3/2}}{2^n}+\frac{q^2\varepsilon}{2^n}+\frac{9q}{2^n}+\frac{27q^2+22q^3}{6\cdot 2^{2n}}+\frac{5q_v}{2^n}\\&\leqslant\frac{13.5q+q^2\varepsilon+5q^{3/2}+5q_v}{2^n}\end{aligned}$$

定理 3 的结论得证!

定理 3 的结果表明, 如果 H 是一个 XU 哈希函数, 即 $\varepsilon=2^{-n}$, 则 EWCDMD 在 nonce-respecting 设置下是可证明抗生日界安全的, 它能够抵抗 $O(2^{2n/3})$ 对手 MAC 查询和 $O(2^n)$对手验证查询(伪造尝试), 即 EWCDMD 确保了 $2n/3$ 比特的认证安全性。与之前 EWCDMD 最优界[10]相比较, 采用细粒度化的拓展的镜像理论证明方法, 更具体更有效的展现了 EWCDMD 的参数广泛范围下紧致安全界。表 2 直观且详细的展示了我们工作的创新与价值。

表 2 EWCDMD 研究结果对比

Table 2 Comparison of EWCDMD Research Results

文献	[10]	本文
证明技术	拓展的镜像理论	拓展的镜像理论
安全性(bit)	n-log67-log n	$2n/3$
界紧致性	不紧致	紧致
适用参数	广泛范围	广泛范围

备注: 适用参数指的是连通分支顶点数 ξ 或者顶点数大于等于 3 的连通分支的总边数 q_c 的适用参数范围。

4.2 应用到级联结构的 EWCDM 方案

令 P_1, P_2 是两个独立的 n 比特长的伪随机置换, N 是一个 nonce-respecting 的 nonce(即要求加密使用的 nonce 都不同), H 是一个 ϵ-AXU 哈希函数, 则从任意比特长的消息 M 到 n 比特长的标签 T 的基于 nonce 的消息认证码 EWCDM 方案如下:

$$T=P_2(P_1(N)\oplus N\oplus H(M))$$

定理 4. 假设对手 **A** 做 q 次 MAC 查询和 q_v 次伪造尝试, 则 EWCDM 方案的 MAC 安全优势为:

$$Adv^{mac}_{EWCDMD}(\mathbf{A})\leqslant\frac{13.5q+q^2\varepsilon+5q^{3/2}+5q_v}{2^n}.$$

证明. 定理 4 的证明过程与定理 3 的证明过程类似, 只有拓展的镜像系统以及坏的脚本事件的定义稍有差异。根据敌手交互查询得到的应答脚本 $\tau=\{(N_1,M_1,T_1),...,(N_q,M_q,T_q),(N_1^{'},M_1^{'},T_1^{'}),...,(N_{q_v}^{'},M_{q_v}^{'},T_{q_v}^{'})\}$, 定义如下包含 q 个仿射等式方程组系统和 q_v 个不等式方程组系统组成的拓展的镜像系统 S:

$$S^{=}:\begin{cases}P_2^{-1}(T_1)\oplus P_1(N_1)=N_1\oplus H(M_1)\\P_2^{-1}(T_2)\oplus P_1(N_2)=N_2\oplus H(M_2)\\\quad\cdots\cdots\\P_2^{-1}(T_q)\oplus P_1(N_q)=N_q\oplus H(M_q)\end{cases}$$

$$S^{\neq}:\begin{cases}P_2^{-1}(T_1^{'})\oplus P_1(N_1^{'})\neq N_1^{'}\oplus H(M_1^{'})\\P_2^{-1}(T_2^{'})\oplus P_1(N_2^{'})\neq N_2^{'}\oplus H(M_2^{'})\\\quad\cdots\cdots\\P_2^{-1}(T_{q_v}^{'})\oplus P_1(N_{q_v}^{'})\neq N_{q_v}^{'}\oplus H(M_{q_v}^{'})\end{cases}$$

令 $X_{a_i}=P_2^{-1}(T_i)$, $X_{b_i}=P_1(N_i)$, $y_i=N_i\oplus H(M_i)$, 由于$N_i\neq N_j$, 因此, $X_{b_i}\neq X_{b_j}$, 这里$1\leqslant i\neq j\leqslant q$。令 $X_{a_{q+i}}=P_2^{-1}(T_i^{'})$, $X_{b_{q+i}}=P_1(N_i^{'})$, $y_{q+i}=$

$N_i^{'} \oplus H(M_i^{'})$, 这里 $1 \leqslant i \leqslant q_v$。由于 P_1, P_2 都是随机选取的, 因此, $X_{a_i} \neq X_{b_j}$, 这里 $1 \leqslant i \neq j \leqslant q+q_v$。则上面拓展的镜像系统可以描述为一个无向带权二部图 $G=<V_1, V_2, E, W>$, 其中

- V_1 是由 $X_{a_1},...,X_{a_{q+q_v}}$ 不重复元素组成的顶点集, V_2 是由集合 $\{X_{b_1},...,X_{b_q}\}$ 和 $X_{b_{q+1}},...,X_{b_{q+q_v}}$ 不重复元素组成的顶点集, 并且 $V_1^{=}$是由 $X_{a_1},...,X_{a_q}$ 不重复元素组成的仿射等式方程组系统的顶点集, $V_2^{=}=\{X_{b_1},...,X_{b_q}\}$。
- $E=E^{=} \cup E^{\neq}=\{e_i=(X_{a_i}, X_{b_i})\}_{i=1}^{q+q_v}$, 其中 $E^{=}=\{e_1,...,e_q\}$ 是仿射等式方程组系统的等边集; $E^{\neq}=\{e_{q+1},...,e_{q+q_v}\}$ 是仿射不等式方程组系统的不等边集。
- $W: E \to \{0,1\}^n$, 对于每一条边 $e_i \in E$, 都有 $W(e_i)=y_i$, 其中 $1 \leqslant i \leqslant q+q_v$。

在真实方案中, 对于任意的 $1 \leqslant i \neq j \leqslant q$, 如果存在 $T_i=T_j$, 即 $X_{a_i}=X_{a_j}$, 则称存在一个碰撞的脚本事件。除此之外, 对于任意的 $1 \leqslant i \neq j \leqslant q$, 如果 $T_i=T_j$ 并且 $N_i \oplus H(M_i)=N_j \oplus H(M_j)$, 则与 $N_i \neq N_j$ 相矛盾。考虑到拓展的镜像系统的约束条件情况, 我们先定义一个 “坏” 的脚本记录。

定义 5 (“坏”的脚本记录). 对于一个脚本记录 τ, 如果 $|T_i=T_j| > \sqrt{q}$ 或者 $T_i=T_j$ 并且 $N_i \oplus H(M_i)=N_j \oplus H(M_j)$, 其中 $1 \leqslant i \neq j \leqslant q$, 那么我们称 τ 是“坏” 的。

令 Γ 表示所有可获得的脚本记录集合, Γ_{bad} 表示所有 “坏”的脚本记录集合, $\Gamma_{good}=\Gamma \setminus \Gamma_{bad}$。下面, 根据 H 系数技术 (引理 1), 给出理想方案中 “坏”的脚本记录发生的概率。

在理想方案中, 根据马尔科夫不等式 $\Pr[X \geqslant a] \leqslant \frac{E(X)}{a}$ 和 ϵ-AXU 哈希函数的定义, 有

$$\begin{aligned}
&\Pr[X_{id} \in \Gamma_{bad}] \\
&= \Pr[|T_i=T_j| \geqslant \sqrt{q}] + \Pr[T_i=T_j, N_i \oplus H(M_i) \\
&= N_j \oplus H(M_j)] \\
&\leqslant \frac{E[|T_i=T_j|]}{\sqrt{q}} + \frac{q^2\varepsilon}{2^n} \leqslant \frac{q^{3/2}}{2^n} + \frac{q^2\varepsilon}{2^n}
\end{aligned}$$

在“好”的脚本记录下, 拓展的镜像系统满足约束条件:

无圈性。由于对于任意的 $1 \leqslant i, j \leqslant q$ 都有 $X_{a_i} \neq X_{b_j}$, 因此, 无向带权图中任意两顶点之间至多只存在一条路径。

连通分支顶点数 ($2\sqrt{q}-1$)-最大。根据 $|T_i=T_j| \leqslant \sqrt{q}-1$ 即 $|X_{a_i}=X_{a_j}| \leqslant \sqrt{q}-1$, 也就是集合 V_1 中相等的顶点数最多为 $\sqrt{q}-1$。因此, 子图 $G^{=}$ 中顶点数大于 2 的所有连通分支的总边数至多为 $2(\sqrt{q}-1)$。结合子图 $G^{=}$的等式连通关系 (连通分支), 可以将顶点集 V 划分为若干个非空子集。根据连通分支是树的性质, 子图 $G^{=}$中连通分支顶点数最多等于 $2\sqrt{q}-1$。

非零路径权。对于任意的 $1 \leqslant i, j \leqslant q$ 都有 $X_{a_i} \neq X_{b_j}$, $X_{b_i} \neq X_{b_j}$, 所以子图 $G^{=}$中不存在任何一条路径 $Path$ 使得 $W(Path)=0$。

非零圈权。 由于对于任意的 $1 \leqslant i, j \leqslant q$ 都有 $X_{a_i} \neq X_{b_j}$, $X_{b_i} \neq X_{b_j}$, 所以图 G 中不存在包含且仅包含一条不等边的圈 C 使得 $W(C)=0$。

假设拓展的镜像系统中 $|V_1|=q'$, $|V_2|=q''$, 因此, 根据拓展的镜像理论的二部图描述定理 2, 真实方案导出的镜像系统解的个数至少是

$$\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)$$

于是, 真实方案在“好”的脚本 τ 下, 除这 r 个随机变量 $\{X_1, \cdots, X_r\}$ 之外的值, 是按照独立随机置换来取值。因此有

$$\begin{aligned}
&\Pr[X_{re}=\tau]=\Pr[P_1, P_2 \leftarrow Perm(n): EWCDM \triangleright \tau] \\
&\geqslant \frac{\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)\cdot(2^n-q')!(2^n-q'')!}{(2^n!)^2} \\
&\geqslant \frac{1}{2^{nq}}\left(1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}\right)
\end{aligned}$$

而理想方案在 “好”的脚本 τ 下, 都是随机选取的, 因此有

$$\Pr[X_{id}=\tau]=\frac{1}{2^{nq}}$$

于是, 对于所有 “好”的脚本 τ, 我们有

$$\frac{\Pr[X_{re}=\tau]}{\Pr[X_{id}=\tau]} \geqslant 1-\frac{9q}{2^n}-\frac{27q^2+22q^3}{6\cdot 2^{2n}}-\frac{5q_v}{2^n}.$$

根据 H 系数技术引理 (引理 1), 有

$$Adv^{mac}_{EWCDM}(\mathbf{A}) \leqslant \frac{q^{3/2}}{2^n}+\frac{q^2\varepsilon}{2^n}+\frac{9q}{2^n}+\frac{27q^2+22q^3}{6\cdot 2^{2n}}+\frac{5q_v}{2^n} \leqslant \frac{13.5q+q^2\varepsilon+5q^{3/2}+5q_v}{2^n}$$

定理 4 的结论得证!

定理 4 的结果表明, 如果 H 是一个 XU 哈希函数, 即 $\varepsilon=2^{-n}$, 则 EWCDM 在 nonce-respecting 设置下是可证明抗生日界安全的, 它能够抵抗 $O(2^{2n/3})$对手 MAC 查询和 $O(2^n)$对手验证查询(伪造尝试), 即 EWCDM 确保了 $2n/3$ 比特的认证安全性。与之前 EWCDM 安全性界[24]相比较, 采用细粒度化的拓展的镜像理论证明方法同样论证了安全性上界, 同时也消除了 Datta 等学者对于广泛范围 q_c 下的安全缺陷问题 [17], 更具体更有效的展现了 EWCDM 的普适性安全界。表 3 更是直观且详细的展示了我们工作的创新与价值。

表 3 EWCDM 研究结果对比

Table 3 Comparison of EWCDM Research Results

文献	[24]	[10]	[17]	本文
证明技术	常用技术	拓展的镜像理论	拓展的镜像理论	拓展的镜像理论
安全性(bit)	$2n/3$	n-log67-log n	$3n/4$	$2n/3$
界紧致性	紧致	不紧致	-	紧致
适用参数	广泛范围	广泛范围	q_c 受限	广泛范围

备注: 适用参数指的是连通分支顶点数 ξ 或者顶点数大于等于 3 的连通分支的总边数 q_c 的适用参数范围。

5 讨论

第 4 部分的两个消息认证码方案 EWCDMD 和 EWCDM 都是基于 2 个伪随机置换构造的, 因此在它们的可证明安全过程中使用的是二变量拓展的镜像理论, 即考虑的是形如

$$S^{=}:\begin{cases} X_{a_1}\oplus X_{b_1}=y_1 \\ X_{a_2}\oplus X_{b_2}=y_2 \\ \cdots\cdots \\ X_{a_q}\oplus X_{b_q}=y_q \end{cases} \quad S^{\neq}:\begin{cases} X_{a_{q+1}}\oplus X_{b_{q+1}}\neq y_{q+1} \\ X_{a_{q+2}}\oplus X_{b_{q+2}}\neq y_{q+2} \\ \cdots\cdots \\ X_{a_{q+q_v}}\oplus X_{b_{q+q_v}}\neq y_{q+q_v} \end{cases}$$

的仿射等式或不等式方程组系统。然而, 消息认证码方案也是可以通过多个独立的伪随机置换进行构造, 例如: 令 M 表示明文消息, T 表示认证标签, $P_1,\ldots,P_r$ 表示 r 个独立的伪随机置换, 消息认证码方案 SUM-MAC 可以表示为

$$T=P_1(M)\oplus P_2(M)\oplus\cdots\oplus P_r(M)$$

Lucks[9]使用所谓的 fair 集合技术给出了该方案的伪随机函数版本的安全性证明, 明确其提供了 $\frac{r}{r+1}\cdot n$ 比特安全性。最近, Dinur[29]使用傅里叶分析技术也给出了该方案的伪随机函数版本的安全性证明, 呈现了 $(r\text{-}0.5)n$ 比特的单用户安全性。如果使用超图来描述的话, q 次 MAC 查询和 q_v 次伪造查询(验证查询)所对应的 r 变量的仿射等式方程组 $S^{=}$ 和不等式方程组 $S^{\neq}$ 的系统(这里称为 r 变量拓展的镜像系统)如下:

$$S^{=}:\begin{cases} X_{1_1}\oplus X_{2_1}\oplus\cdots\oplus X_{r_1}=T_1 \\ X_{1_2}\oplus X_{2_2}\oplus\cdots\oplus X_{r_2}=T_2 \\ \cdots\cdots \\ X_{1_q}\oplus X_{2_q}\oplus\cdots\oplus X_{r_q}=T_q \end{cases}$$

$$S^{\neq}:\begin{cases} X_{1_{q+1}}\oplus X_{2_{q+1}}\oplus\cdots\oplus X_{r_{q+1}}\neq T_{q+1} \\ X_{1_{q+2}}\oplus X_{2_{q+2}}\oplus\cdots\oplus X_{r_{q+2}}\neq T_{q+2} \\ \cdots\cdots \\ X_{1_{q+q_v}}\oplus X_{2_{q+q_v}}\oplus\cdots\oplus X_{r_{q+q_v}}\neq T_{q+q_v} \end{cases}$$

这里 $X_{1_i}=P_1(M_i),\ldots,X_{r_i}=P_r(M_i)$, 其中 $1\leqslant i,\ j\leqslant q+q_v$。每个 r 变量的仿射等式都可以使用 r–1 个二变量的仿射方程组来描述, 则敌手做 q 次 MAC 查询的系统对应一个由 $(r-1)q$ 个方程 mq 个未知数组成的等式方程组。但是敌手做 q_v 次伪造查询(验证查询)所对应的 r 变量的仿射不等式方程组使用二变量的仿射不等式方程组来描述的情况就非常复杂了, 因此不完全满足二变量拓展的镜像系统的应用要求。这种方法本质上是转化为了二变量拓展的镜像理论, 是否可以将二变量拓展的镜像理论推广到多变量拓展的镜像理论, 也给出超图描述形式以及相应的解数计数表达式, 以快速适应此类基于多个独立伪随机置换构造的消息认证码方案呢? 这里我们将如何推广到多变量拓展的镜像理论超图解数计数上界以及如何使用多变量拓展的镜像理论证明 SUM-MAC 方案确保了 $\frac{r}{r+1}\cdot n$ 比特的安全性作为开放性问题遗留下来以期进一步讨论与研究。

6 结论

本文聚焦拓展的镜像理论的图论描述及其在抗生日界安全的消息认证码的可证明安全中的应用。论文首先使用图论语言描述了二变量拓展的镜像理

论, 并给出了其图论语言下的约束条件和更广泛范围下的普适性计数结果。然后, 将其应用到基于两个独立伪随机置换的抗生日界安全的消息认证码的安全性证明中, 证明了基于两个独立伪随机置换的并联结构和级联结构的消息认证码都是 $2n/3$ 比特安全的。基于两个独立伪随机置换设计的消息认证码方案的可证明安全依赖于二变量拓展的镜像理论的图理论, 是否可以将其推广到基于多个独立伪随机置换的消息认证码方案的可证明安全中, 从而形成多变量拓展的镜像理论的超图理论呢，由于推广方案分析相对较为复杂, 这里作为开放性问题以待进一步完善。论文的工作增强了广泛参数下的镜像理论, 对于消息认证码方案的设计及其可证明安全理论分析都具有极其重要的学术理论价值和实践指导意义。

参考文献

[1] Patarin J. On Linear Systems of Equations with Distinct Variables and Small Block Size[C]. *Information Security and Cryptology - ICISC 2005*, 2006: 299-321.

[2] Patarin J. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography [EB/OL]. 2010: IACR Cryptol. ePrint Arch., 287.

[3] Patarin J. Mirror Theory and Cryptography[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2017, 28(4): 321-338.

[4] Nachef V, Patarin J, Volte E. Introduction to mirror theory [M]. Berlin: Springer-Verlag, 2017: 203-221.

[5] Dutta A, Nandi M, Saha A. Proof of Mirror Theory for Ξmax = 2[J]. *IEEE Transactions on Information Theory*, 2022, 68(9): 6218-6232.

[6] Chen Y L. A Modular Approach totheSecurity Analysis OfTwo-Permutation Constructions[C]. *Advances in Cryptology-ASIACRYPT 2022*, 2022: 379-409.

[7] Cogliati B, Dutta A, Nandi M, et al. Proof of Mirror Theory for a Wide Range of $$\xi_{\max}$$[M]. Advances in Cryptology-EUROCRYPT 2023. Cham: Springer Nature Switzerland, 2023: 470-501.

[8] Bellare M, Krovetz T, Rogaway P. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-Invertible[C]. *Advances in Cryptology — EUROCRYPT'98*, 1998: 266-280.

[9] Lucks S. The Sum of PRPS Is a Secure PRF[C]. *Advances in Cryptology — EUROCRYPT 2000*, 2000: 470-484.

[10] Mennink B, Neves S. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory[C]. *Advances in Cryptology-CRYPTO 2017*, 2017: 556-583.

[11] Chen Y L, Lambooij E, Mennink B. How to Build Pseudorandom Functions from Public Random Permutations[C]. *Advances in Cryptology-CRYPTO 2019*, 2019: 266-293.

[12] Dutta A, Nandi M, Talnikar S. Permutation Based EDM: An Inverse Free BBB Secure PRF[J]. *IACR Transactions on Symmetric Cryptology*, 2021: 31-70.

[13] Cogliati B, Ethan J, Lallemand V, et al. CTET+: A beyond-birthday-bound secure tweakable enciphering scheme using a single pseudorandom permutation [J]. *IACR Transactions on Symmetric Cryptology*, 2021(4): 1-35.

[14] Cogliati B. Tweaking a Block Cipher: Multi-User Beyond-Birthday-Bound Security in the Standard Model[J]. *Designs, Codes and Cryptography*, 2018, 86(12): 2747-2763.

[15] Bao Z Z, Hwang S, Inoue A, et al. XOCB: Beyond-Birthday-Bound Secure Authenticated Encryption Mode WithRate-One Computation[C]. *Advances in Cryptology – EUROCRYPT 2023*, 2023: 532-561.

[16] Datta N, Dutta A, Nandi M, et al. Encrypt or Decrypt? to Make a Single-Key beyond Birthday Secure Nonce-Based MAC[C]. *Advances in Cryptology – CRYPTO 2018*, 2018: 631-661.

[17] Datta N, Dutta A, Dutta K. Improved security bound of (E/D)WCDM [J]. *IACR Transactions on Symmetric Cryptology*, 2021: 138-176.

[18] Chakraborti A, Nandi M, Talnikar S, et al. On the composition of single-keyed tweakable Even-Mansour for achieving BBB security [J]. *IACR Transactions on Symmetric Cryptology*, 2020: 1-39.

[19] Choi W, Inoue A, Lee B, et al. Highly secure nonce-based MACs from the sum of tweakable block ciphers [J]. *IACR Transactions on Symmetric Cryptology*, 2020(4): 39-70.

[20] Shen Y B, Wang L, Gu D W, et al. Revisiting the Security of DbHtS MACs: Beyond-Birthday-Bound in the Multi-User Setting[C]. *Advances in Cryptology-CRYPTO 2021*, 2021: 309-336.

[21] Chen Y L, Dutta A, Nandi M. Multi-User BBB Security of Public Permutations Based MAC[J]. *Cryptography and Communications*, 2022, 14(5): 1145-1177.

[22] Dutta A, Nandi M, Talnikar S. Beyond Birthday Bound Secure MAC in Faulty Nonce Model[C]. *Advances in Cryptology – EUROCRYPT 2019*, 2019: 437-466.

[23] Dutta A, Jha A, Nandi M. Tight security analysis of EHTM MAC [J]. *IACR Transactions on Symmetric Cryptology*, 2017(3): 130-150.

[24] Cogliati B, Seurin Y. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC[C]. *Advances in Cryptology -CRYPTO 2016*, 2016: 121-149.

[25] Shen Y B, Wang L. On Beyond-Birthday-Bound Security: Revisiting the Development of ISO/IEC 9797-1 MACs[J]. *IACR Transactions on Symmetric Cryptology*, 2019: 146-168.

[26] Shen Y B, Sibleyras F. Key-Reduced Variants of 3kf9 with Beyond-Birthday-Bound Security[M]. Advances in Cryptology-ASIACRYPT 2022. Cham: Springer Nature Switzerland, 2022: 525-554.

[27] Patarin J. The “Coefficients H” Technique[C]. *Selected Areas in Cryptography*, 2009: 328-345.

[28] Wu W L, Feng D G, Zhang W T. Design and analysis of block cipher[M]. 2nd ed. Beijing: Tsinghua University Press, 2009: 355-356.
(吴文玲, 冯登国, 张文涛. 分组密码的设计与分析[M]. 2版. 北京: 清华大学出版社, 2009: 355-356.)

[29] Dinur I. Tight Indistinguishability Bounds fortheXOR ofIndependent Random Permutations byFourier Analysis[C]. *Advances in Cryptology-EUROCRYPT 2024*, 2024: 33-62.

张平 于 2018 年在中国科学技术大学信息与通信工程专业获得工学博士学位。现任南京邮电大学计算机学院、软件学院、网络空间安全学院讲师, 硕士生导师, CCF 会员。研究领域为信息安全、密码学。研究兴趣包括: 对称密码的设计与分析、抗量子计算对称密码设计与分析。Email: zhgp@njupt.edu.cn

秦佳琦 于 2023 年在南京邮电大学信息安全专业获得学士学位。现任南京邮电大学计算机学院、软件学院、网络空间安全学院密码理论与应用课题组科研助理。研究领域为信息安全、密码学。研究兴趣包括: 对称密码的设计与分析、抗量子计算对称密码设计与分析。Email: b19031025@njupt.edu.cn