中国科学 : 信息科学 2025 年 第 55 卷 第 5 期: 1007–1032
SCIENTIA SINICA Informationis
论文

基于可调 Even-Mansour 密码实例构造超生日界安全的可调密码本原

张平[1,2], 罗宜元[3*]

1. 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 210023
2. 四川省先进密码技术与系统安全重点实验室, 成都 610225
3. 惠州学院计算机科学与工程学院, 惠州 516007
* 通信作者. E-mail: luoyy@hzu.edu.cn

收稿日期: 2024–11–04; 修回日期: 2024–12–25; 接受日期: 2024–12–27; 网络出版日期: 2024–04–30

国家自然科学基金 (批准号: 62072207, U23B2002, 62272238, 61902195)、广东省基础与应用基础研究基金 (批准号: 2022A1515140090)、广东省教育厅重点领域专项 (批准号: 2024ZDZX1025) 和四川省先进密码技术与系统安全重点实验室开放课题 (批准号: SKLACSS-202315) 资助项目

摘要 近年来, 超生日界安全的密码本原备受关注. 可调密码本原作为传统密码本原的拓展, 在密码算法或网络安全通信协议中也发挥着重要作用. 然而, 其超生日界安全的设计方案却鲜有出现. 因此, 本文关注超生日界安全的可调密码本原设计与分析, 从基于公共置换的可调 Even-Mansour 密码出发, 设计基于可调 Even-Mansour 密码实例的超生日界安全的可调伪随机函数和强可调伪随机置换. 首先, 针对陈玉龙提出的随机置换模型下的拓展镜像理论限制了不同随机置换查询的差异性和交集为空的问题, 本文对不同随机置换做了差异化改进查询以及交集非空的拓展, 给出了更一般性的适配拓展镜像理论解的上界. 然后, 基于两个可调 Even-Mansour 密码实例的并级联结构分别构造了超生日界安全的可调伪随机函数和强可调伪随机置换, 并采用改进的拓展镜像理论分别给出了可证明安全结果. 最后, 讨论了基于多个可调 Even-Mansour 密码实例的并级联结构来构造超生日界安全的对称密码本原及其所依赖的基于多变量的镜像系统超图理论以及基于单置换单密钥最小结构且域保持的超生日界安全对称密码本原设计思路. 本文的工作丰富了镜像理论和密码本原, 同时对于构建可证明超生日界安全的对称密码方案具有重要的理论研究意义与实践指导价值.

关键词 超生日界安全, 可调密码本原, 可调 Even-Mansour 密码, 镜像理论, 随机置换模型

1 前言

密码本原是设计密码方案的核心, 包括随机函数、伪随机函数、随机置换、伪随机置换、强伪随机置换等. 所谓伪随机函数 (伪随机置换、强伪随机置换), 就是它与随机函数 (随机置换) 在计算复杂度意义上不可区分. 分组密码作为常用伪随机函数、伪随机置换、强伪随机置换本原被广泛应用于安全

引用格式: 张平, 罗宜元. 基于可调 Even-Mansour 密码实例构造超生日界安全的可调密码本原. 中国科学: 信息科学, 2025, 55: 1007–1032, doi: 10.1360/SSI-2024-0328
Zhang P, Luo Y Y. Beyond-birthday-bound (BBB) secure tweakable cryptographic primitives based on tweakable Even-Mansour cipher instances. Sci Sin Inform, 2025, 55: 1007–1032, doi: 10.1360/SSI-2024-0328

有效密码方案的设计及其可证明安全分析中. 可调分组密码是分组密码的拓展, 它在输入时引入了一个额外的参数调柄, 使得分组密码的使用范围更加壮大. 与其相依存的本原即可调密码本原, 包括可调随机函数、可调伪随机函数、可调随机置换、可调伪随机置换、强可调伪随机置换等也是传统密码本原的拓展. 可调密码主要始于磁盘扇区加密、保序加密等数据存储加密中, 后来在各工作模式中也有广泛使用, 如加密模式、消息认证码、认证加密以及相关的网络通信协议 [1].

传统密码本原的设计与分析主要围绕伪随机函数、伪随机置换、强伪随机置换. 从伪随机函数可以设计伪随机置换、强伪随机置换, 如使用 3 轮 Feistel 密码可以构造一个安全的伪随机置换, 使用 4 轮 Feistel 密码可以构造一个安全的强伪随机置换等 [2,3]. 从伪随机置换或公开随机置换也可以构造伪随机函数, 如使用伪随机置换 – 伪随机函数转化引理, 可以将伪随机置换转化为伪随机函数, 但这会引入生日界瓶颈 [1,4]. 所谓生日界, 即对于分组长度为 n 比特的密码算法, 由于伪随机置换与伪随机函数转化引理以及其以工作模式的方式使用, 其只能提供最多 $n/2$ 比特的安全性. 如高级加密标准 AES 算法, 其分组长度是 128 比特, 被用于加密、认证以及认证加密工作模式时, 安全性强度降为 64 比特. 再如轻量级密码 PRESENT 算法, 其分组长度是 64 比特, 被用于加密、认证以及认证加密工作模式时, 安全性强度降为 32 比特, 这在正常的环境下都不可以被使用, 往往应用在一些对安全强度要求较低的轻量级环境中. 于是, 提出了超生日界安全的设计思想. 超生日界安全指的就是安全性强度高于通常生日界, 具体来说就是, 对于分组长度为 n 比特的密码算法, 它以工作模式的方式使用时, 能够提供超越 $n/2$ 比特的安全性. 特别地, 如果对于分组长度为 n 比特的密码算法, 它以工作模式的方式使用时, 能够提供 n 比特的安全性, 那么则称最优安全. 将多个伪随机置换或公开随机置换的并联和或者级联接或者截断拼接等方法来生成伪随机函数或强伪随机置换, 从而实现超生日界安全的密码本原设计是使用最为广泛的方法 [5~12].

镜像理论在超生日界安全密码本原的可证明安全理论中有着重要的应用 [13~20]. 镜像理论是 Patarin 提出的一种计算仿射等式和不等式方程组系统解的个数的重要数学工具. 起初命名为 $P_i \oplus P_j$ 定理, 因为其最初来源于 “两个独立的分组密码的异或和是一个超生日界安全的伪随机函数” 的安全性分析. 镜像理论关注的是 $v \oplus y = \lambda$ 为形式的未知数仿射等式方程组系统, 其中 v 和 y 是两个未知数, λ 是已知值. 目的是确定未知数的可能解的数量的下界 [13~17]. 后来考虑到未知数仿射等式方程组系统中可能也存在形如 $v \oplus y \neq \lambda$ 的方程系统, Datta 等 [18] 进一步纳入不等式仿射方程组到镜像系统. 考虑到传统的拓展镜像理论只是针对双变量仿射等式和仿射不等式方程组镜像系统进行解的个数界定, 陈玉龙 [19] 进一步推广了这个情况, 提出了既包含双变量仿射等式和仿射不等式方程组, 又纳入了单变量仿射等式 $v = \lambda$ 和 $y = \lambda$ 在内的随机置换模型下的拓展镜像理论, 这进一步拓展了镜像理论在超生日界安全的密码本原方案设计与分析中的研究.

类似地, 可调密码本原的设计与分析主要围绕可调伪随机函数、可调伪随机置换、强可调伪随机置换. 可调伪随机函数可以用来构造可调伪随机置换和强可调伪随机置换, 可调伪随机置换也可以用来构造可调伪随机函数. 由于可调密码本原是在传统密码本原之上引入了一个调柄, 因此转化方法基本一样. 除此之外, 传统密码本原也可以用来设计可调密码本原. 如使用伪随机函数、伪随机置换、强伪随机置换来设计可调伪随机函数、可调伪随机置换、强可调伪随机置换. 基于 XE, XEX, XEX*, XPX, MEM 等结构可以将伪随机函数、伪随机置换、强伪随机置换、公开随机置换转化为可调伪随机函数、可调伪随机置换、强可调伪随机置换等, 但均存在生日界瓶颈 [21~23]. 目前基于超生日界安全的可调密码本原设计方案比较少 [24,25].

本文关注超生日界安全的可调密码本原设计. 从基于公开随机置换的可调 Even-Mansour 密码出发, 设计基于可调 Even-Mansour 密码实例的超生日界安全的可调伪随机函数和强可调伪随机置换. 首先, 针对陈玉龙 [19] 提出的随机置换模型下的拓展镜像理论应用受限的问题, 提出了改进的随机置换模型下的拓展镜像理论. 陈玉龙 [19] 考虑了 p 个一致的 v 和 y 单变量仿射等式, 这限制了随机置换查询的差异性. 除此之外, 还要求集合 $V^p = \{v\}$ 和 $Y^p = \{y\}$ 不相交, 即 $V^p \cap Y^p = \emptyset$, 这局限了拓展镜

表 1　拓展镜像理论的适用范围.

Table 1　Applicable scope of extended mirror theory.

Applicable scope	Traditional mirror theory [13~18]	Chen's mirror theory [19]	Improved mirror theory
System of bi-variate equations	$v \oplus y = \lambda$	$v \oplus y = \lambda$	$v \oplus y = \lambda$
System of bi-variate non-equations	$v \oplus y \neq \lambda'$	$v \oplus y \neq \lambda'$	$v \oplus y \neq \lambda'$
System of uni-variate equations	–	$\lvert\{v = \lambda\}\rvert = \lvert\{y = \lambda\}\rvert$	$\lvert\{v = \lambda\}\rvert \neq \lvert\{y = \lambda\}\rvert$
$\{v\} \cap \{y\}$	$\emptyset$	$\emptyset$	$\neq \emptyset$
Graph	Bipartite graph	Bipartite graph	General graph
Traditional cryptographic primitives	Yes	Yes	Yes
Tweakable cryptographic primitives	–	Yes	Yes

表 2　设计方案与以前方案的结果比较.

Table 2　Comparison between the designed schemes and the previous schemes.

Scheme	Primitive	Structure	Keys	Tweaks	Permutations	Method	Security	Reference
pEDM	PRF	Cascade	2	0	2	Chen's mirror theory	$2n/3$-bit	[19]
SoEM22	PRF	Summation	2	0	2	Traditional technique	$2n/3$-bit	[9]
SoTEM	TPRF	Summation	2	1	2	Improved mirror theory	$2n/3$-bit	Subsection 4.1
mSoTEM	TPRF	Summation	1	2	1	Improved mirror theory	$2n/3$-bit	Section 5
EM2	SPRP	Cascade	2	0	2	Traditional technique	$2n/3$-bit	[26]
2-EM	SPRP	Cascade	1	0	1	Traditional technique	$2n/3$-bit	[11]
TEM2	STPRP	Cascade	2	1	2	Chen's mirror theory	$2n/3$-bit	[19]
2-TEM	STPRP	Cascade	2	1	1	Traditional technique	$2n/3$-bit	[12]
CoTEM	STPRP	Cascade	2	1	2	Improved mirror theory	$2n/3$-bit	Subsection 4.2

像理论的应用场景. 因此, 为适应随机置换的差异查询和体现更广泛的应用空间, 我们进一步对随机置换查询做差异化改进, 分别考虑 p_1 个 v 单变量仿射等式和 p_2 个 y 单变量仿射等式, 同时考虑集合 $V^{p_1} = \{v\}$ 和 $Y^{p_2} = \{y\}$ 有交集, 即 $V^{p_1} \cap Y^{p_2} \neq \emptyset$, 并给出了更一般性的适配拓展镜像理论解的上界. 比较所有拓展镜像理论适用范围并总结如表 1 [13~19] 所示.

然后, 从基于公共置换的可调 Even-Mansour 密码出发, 分别基于可调 Even-Mansour 密码实例的并级联结构 (并联和以及级联接两种结构) 设计了支持超生日界安全的可调伪随机函数 SoTEM 和强可调伪随机置换 CoTEM. 同时, 基于新改进的拓展镜像理论证明了新设计的可调密码本原都是 $2n/3$ 比特紧致安全的. 最后, 本文讨论了超生日界安全的可调密码本原的设计与分析思路, 留下了推广二变量的拓展镜像系统到多变量的拓展镜像系统超图理论以及设计基于单个公开置换和单个密钥、具有域保持和最小结构、超生日界安全的可调密码本原开放性问题. 设计方案与以前方案的结果比较如表 2 [9, 11, 12, 19, 26] 所示.

本文结构安排如下: 第 2 节是基础知识介绍; 第 3 节给出了改进的拓展镜像理论的图论描述形式以及计数结果; 第 4 节给出了基于两个可调 Even-Mansour 密码实例构造的超生日界安全的可调伪随机函数和可调伪随机置换, 并基于改进的拓展镜像理论给出了可证明安全的结果; 第 5 节讨论了基于多个可调 Even-Mansour 密码实例构造的方案的超生日界安全及其所依赖的多变量的拓展镜像系统超图理论; 第 6 节是全文总结.

2　基础知识

基本符号. 令 $\{0,1\}^n$ 表示长度为 n 的比特串的集合, $\{0,1\}^*$ 表示所有比特串的集合, $|X|$ 表示比

特串 X 的比特长度或集合 X 的元素个数, $X||Y$ 表示两个比特串 X 和 Y 的连接, $X\oplus Y$ 表示两个比特串 X 和 Y 的异或, $x\xleftarrow{\$}X$ 表示从集合 X 中随机选取一个 x, $\mathrm{Func}(m,n)$ 表示从 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的所有函数的集合 (当 $m=n$ 时, 简记作 $\mathrm{Func}(n)$), $\mathrm{Perm}(n)$ 表示 $\{0,1\}^n$ 上所有置换的集合. 令 Γ 表示调柄空间, $\widetilde{\mathrm{Func}}(\Gamma,m,n):\Gamma\times\{0,1\}^m\to\{0,1\}^n$ 表示从 $\Gamma\times\{0,1\}^m$ 到 $\{0,1\}^n$ 的所有函数的集合 (当 $m=n$ 时, 简记作 $\widetilde{\mathrm{Func}}(\Gamma,n)$), $\widetilde{\mathrm{Perm}}(\Gamma,n):\Gamma\times\{0,1\}^n\to\{0,1\}^n$ 表示从 $\Gamma\times\{0,1\}^n$ 到 $\{0,1\}^n$ 的所有置换的集合. 令 $a\geqslant b\geqslant 1$ 为整数, $(a)_b$ 表示 $a\cdot(a-1)\cdots(a-b+1)$. 令 $\mathcal{A}$ 是一个确定性敌手, O 是一个预言机, 则 $\mathcal{A}^O=1$ 表示对手 $\mathcal{A}$ 与预言机 O 交互之后, 输出 1. x^{*q} 表示 q 元组 $(x_1,x_2,\ldots,x_q)$, 令 $\mu(x^{*q},x')$ 表示 $x'\in x^{*q}$ 的多重数.

基于公开置换的可调伪随机函数和可调伪随机置换. 令 $P\xleftarrow{\$}\mathrm{Perm}(n)$ 是一个公开随机置换, 基于公开置换 P 的可调函数族 $\widetilde{E}:\{0,1\}^k\times\Gamma\times\{0,1\}^m\to\{0,1\}^n$ 的每个实例 $\widetilde{E}_K^t$ 都是从 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的函数, 其中 $K\in\{0,1\}^k$ 和 $t\in\Gamma$. 如果 $\widetilde{R}\xleftarrow{\$}\widetilde{\mathrm{Func}}(\Gamma,m,n)$, 则称 $\widetilde{R}$ 是一个可调随机函数. 对任意的对手 $\mathcal{A}$, 它可以查询 $\widetilde{E}$ 以及公开置换及其逆置换 $P^{\pm}$, 定义

$$\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprf}}(\mathcal{A})=\left|\Pr\left[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{\widetilde{E}_K;P^{\pm}}=1\right]-\Pr\left[\widetilde{R}\xleftarrow{\$}\widetilde{\mathrm{Func}}(\Gamma,m,n):\mathcal{A}^{\widetilde{R};P^{\pm}}=1\right]\right|$$

为对手 $\mathcal{A}$ 区分可调函数族 $\widetilde{E}$ 和可调随机函数 $\widetilde{R}$ 的概率优势, 即可调伪随机函数优势.

令 $\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprf}}(q,p)=\max_{\mathcal{A}}\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprf}}(\mathcal{A})$, 其中 q 为询问可调函数族次数, p 为询问公开置换 P 次数. 如果 $\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprf}}(q,p)$ 是一个可以忽略的量, 则称 $\widetilde{E}$ 是一个安全的可调伪随机函数 (tweakable pseudo-random function, TPRF).

基于公开置换 P 的可调置换族 $\widetilde{E}:\{0,1\}^k\times\Gamma\times\{0,1\}^n\to\{0,1\}^n$ 的每个实例 $\widetilde{E}_K^t$ 都是从 $\{0,1\}^n$ 到 $\{0,1\}^n$ 的置换. 如果 $\widetilde{P}\xleftarrow{\$}\widetilde{\mathrm{Perm}}(\Gamma,n)$, 则称 $\widetilde{P}$ 是一个可调随机置换. 对任意的对手 $\mathcal{A}$, 它可以查询 $\widetilde{E}$ 或 $\widetilde{E}_K^{\pm}$ 以及公开置换及其逆置换 $P^{\pm}$, 定义

$$\begin{aligned}\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprp}}(\mathcal{A})&=\left|\Pr\left[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{\widetilde{E}_K;P^{\pm}}=1\right]-\Pr\left[\widetilde{P}\xleftarrow{\$}\widetilde{\mathrm{Perm}}(\Gamma,n):\mathcal{A}^{\widetilde{P};P^{\pm}}=1\right]\right|,\\ \mathrm{Adv}_{\widetilde{E}}^{\mathrm{stprp}}(\mathcal{A})&=\left|\Pr\left[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{\widetilde{E}_K^{\pm};P^{\pm}}=1\right]-\Pr\left[\widetilde{P}\xleftarrow{\$}\widetilde{\mathrm{Perm}}(\Gamma,n):\mathcal{A}^{\widetilde{P}^{\pm};P^{\pm}}=1\right]\right|\end{aligned}$$

为对手 $\mathcal{A}$ 区分可调置换族 $\widetilde{E}$ 和可调随机置换 $\widetilde{P}$ 的概率优势, 即可调伪随机置换或强可调伪随机置换优势. 令 $\mathrm{Adv}_{\widetilde{E}}^{(\mathrm{s})\mathrm{tprp}}(q,p)=\max_{\mathcal{A}}\mathrm{Adv}_{\widetilde{E}}^{(\mathrm{s})\mathrm{tprp}}(\mathcal{A})$, 其中 q 为询问可调置换族次数, p 为询问公开置换 P 次数. 如果 $\mathrm{Adv}_{\widetilde{E}}^{\mathrm{tprp}}(q,p)$ 是一个可以忽略的量, 则称 $\widetilde{E}$ 是一个安全的可调伪随机置换 (tweakable pseudo-random permutation, TPRP). 如果 $\mathrm{Adv}_{\widetilde{E}}^{\mathrm{stprp}}(q,p)$ 是一个可以忽略的量, 则称 $\widetilde{E}$ 是一个安全的强可调伪随机置换 (strong tweakable pseudo-random permutation, STPRP).

特别地, 如果不考虑调柄空间, 则可调伪随机函数 TPRF (可调伪随机置换 TPRP、强可调伪随机置换 STPRP) 将退化成伪随机函数 PRF (伪随机置换 PRP、强伪随机置换 SPRP).

泛哈希 (Hash) 函数. 令 $\mathcal{K}$ 是一个哈希密钥空间, $\mathcal{X}$ 是一个有限输入集以及 $n\geqslant 1$ 是一个整数. 如果一个哈希函数 $h:\mathcal{K}\times\mathcal{X}\to\{0,1\}^n$ 满足

(1) ϵ_1-almost uniform (AU), 即对于任意输入 $x\in\mathcal{X}$ 和输出 $a\in\{0,1\}^n$ 都有 $\Pr[K\xleftarrow{\$}\mathcal{K}:h_K(x)=a]\leqslant\epsilon_1$;

(2) ϵ_2-almost XOR universal (AXU), 即对于任意两个不同的输入 $x\neq x'\in\mathcal{X}$ 和输出 $a\in\{0,1\}^n$ 都有 $\Pr[K\xleftarrow{\$}\mathcal{K}:h_K(x)\oplus h_K(x')=a]\leqslant\epsilon_2$;

则称 h 是 ϵ_1-AU 且 ϵ_2-AXU 哈希函数. 特别地, 如果 $\epsilon_1=2^{-n}$, 称 h 是均匀哈希函数; 如果 $\epsilon_2=2^{-n}$, 称 h 是 XU 哈希函数.

H 系数技术. H 系数技术是 Patarin 最早提出来的, 用于界定敌手攻击一个密码方案的优势上界 [27]. 假设一个确定性敌手 $\mathcal{A}$ 来攻击密码方案. 它能查询真实的密码方案 Π 和理想的密码方案 F 以及公共置换 P 和它的逆 P^{-1}, 并试图区分这两个系统 $(\Pi;P^{\pm})$ 和 $(F;P^{\pm})$. 将 $\mathcal{A}$ 与真实的密码方案 Π

和理想的密码方案 F 交互查询 q 次的输入输出对记作一个脚本 $\tau_q=\{(t_1,x_1,y_1),\ldots,(t_q,x_q,y_q)\}$, 与公共置换 P 和它的逆 P^{-1} 交互查询 p 次的输入输出对记作一个脚本 $\tau_p=\{(u_1,v_1),\ldots,(u_p,v_p)\}$, 并记 $\tau=(\tau_q,\tau_p)$. 令 $X_{\rm re}$ 和 $X_{\rm id}$ 分别表示 $\mathcal{A}$ 与真实系统 $(\Pi;P^{\pm})$ 和理想系统 $(F;P^{\pm})$ 交互之后脚本的概率分布. 如果理想系统的脚本概率分布大于 0, 即 $\Pr[X_{\rm id}=\tau]>0$, 我们就称这个脚本是可获得的. 将所有可获得的脚本集合记作 Ω. 于是 H 系数技术引理描述如下.

引理1 (H 系数技术)　考虑所有可获得脚本集合 Ω 的一个划分 $\Omega=\Omega_{\rm good}\cup\Omega_{\rm bad}$. 如果存在 $\alpha\geqslant 0$ 使得 $\Pr[X_{\rm id}\in\Omega_{\rm bad}]\leqslant\alpha$, 并且, 对于任意的好的脚本 $\tau\in\Omega_{\rm good}$, 存在 $\beta\geqslant 0$, 都有

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

则敌手 $\mathcal{A}$ 攻击密码方案 Π 的优势为 $\mathrm{Adv}_{\Pi}(\mathcal{A})=|\Pr[\mathcal{A}^{\Pi;P^{\pm}}=1]-\Pr[\mathcal{A}^{F;P^{\pm}}=1]|\leqslant\alpha+\beta$.

预言机 O 扩展脚本 τ.　令 $\tau_q=\{(t_1,x_1,y_1),\ldots,(t_q,x_q,y_q)\}$ 是敌手与预言机 O 交互查询 q 次得到的输入输出脚本. 如果对于所有的 $i=1,\ldots,q$ 都有 $O(t_i,x_i)=y_i$, 则称预言机 O 扩展脚本 τ_q, 记作 $O\vdash\tau_q$.

3　改进的随机置换模型下的拓展镜像理论

陈玉龙 [19] 提出的随机置换模型下的拓展镜像理论纳入了随机置换查询, 考虑了 p 个一致的 v 和 y 单变量仿射等式, 这限制了随机置换查询的差异性. 除此之外, 还要求集合 $V^p=\{v\}$ 和 $Y^p=\{y\}$ 不相交, 即 $V^p\cap Y^p=\emptyset$, 这使得计算解的个数下界可以继续使用二部图理论进行, 但这同时也局限了拓展镜像理论的应用场景. 因此, 为适应随机置换的差异查询和体现更广泛的应用空间, 我们进一步对随机置换查询做差异化改进, 分别考虑 p_1 个 v 单变量仿射等式和 p_2 个 y 单变量仿射等式, 同时考虑集合 V^{p_1} 和 Y^{p_2} 有交集, 即 $V^{p_1}\cap Y^{p_2}\neq\emptyset$.

定义1 (改进的随机置换模型下的拓展镜像理论的方程描述)　给定整数 $q_m,q_a,p_1,p_2\geqslant 1$ 以及 $1\leqslant q_V^{p_1}\leqslant q_m+q_a+p_1, 1\leqslant q_Y^{p_2}\leqslant q_m+q_a+p_2, 1\leqslant\alpha\leqslant q_m/2$. 令 $V^{p_1}=\{v_1,\ldots,v_{q_V^{p_1}}\}$ 表示 $q_V^{p_1}$ 个两两不同的未知数组成的集合, $Y^{p_2}=\{y_1,\ldots,y_{q_Y^{p_2}}\}$ 表示 $q_Y^{p_2}$ 个两两不同的未知数组成的集合, 并且 $|V^{p_1}\cap Y^{p_2}|=\alpha$. $\lambda_1,\ldots,\lambda_{q_m},\lambda'_1,\ldots,\lambda'_{q_a}$ 表示已知常数. 假设存在两个下标索引满射 $\psi_V^{p_1}$ 和 $\psi_Y^{p_2}$ 分别映射集合 V^{p_1} 和 Y^{p_2} 中元素下标, 即

$$\psi_V^{p_1}:\{I_1,\ldots,I_{q_m+p_1},J_1,\ldots,J_{q_a}\}\to\{1,\ldots,q_V^{p_1}\},$$
$$\psi_Y^{p_2}:\{I_1,\ldots,I_{q_m+p_2},J_1,\ldots,J_{q_a}\}\to\{1,\ldots,q_Y^{p_2}\},$$

则包含 q_m 个二变量仿射等式方程组系统 $\mathcal{E}_m$ 和 q_a 个二变量仿射不等式方程组系统 $\mathcal{E}_a$, 同时容纳 p_1+p_2 个单变量仿射等式方程组系统 $\mathcal{E}_{p_1}\cup\mathcal{E}_{p_2}$ 的随机置换模型下的拓展镜像系统 $\mathcal{E}^{p_1,p_2}=\mathcal{E}_m\cup\mathcal{E}_{p_1}\cup\mathcal{E}_{p_2}\cup\mathcal{E}_a$ 可以表示为

$$\mathcal{E}_m:\begin{cases}v_{I_1}\oplus y_{I_1}=\lambda_1,\\ v_{I_2}\oplus y_{I_2}=\lambda_2,\\ \quad\vdots\\ v_{I_{q_m}}\oplus y_{I_{q_m}}=\lambda_{q_m},\end{cases}\quad\mathcal{E}_{p_1}:\begin{cases}v_{I_{q_m+1}}=\lambda_{q_m+1},\\ v_{I_{q_m+1}}=\lambda_{q_m+2},\\ \quad\vdots\\ v_{I_{q_m+p_1}}=\lambda_{q_m+p_1},\end{cases}\quad\mathcal{E}_{p_2}:\begin{cases}y_{I_{q_m+1}}=\lambda_{q_m+p_1+1},\\ y_{I_{q_m+1}}=\lambda_{q_m+p_1+2},\\ \quad\vdots\\ y_{I_{q_m+p_2}}=\lambda_{q_m+p_1+p_2},\end{cases}\quad\mathcal{E}_a:\begin{cases}v_{J_1}\oplus y_{J_1}\neq\lambda'_1,\\ v_{J_2}\oplus y_{J_2}\neq\lambda'_2,\\ \quad\vdots\\ v_{J_{q_a}}\oplus y_{J_{q_a}}\neq\lambda'_{q_a},\end{cases}$$

其中对于 $1\leqslant i\leqslant q_m+p_1, 1\leqslant i'\leqslant q_m+p_2$, $1\leqslant j\leqslant q_a$ 和 $1\leqslant k\leqslant q_m+p_1+p_2$ 都有 $v_{I_i},v_{J_j},y_{I'_i},y_{J_j}$ 是未知数且 λ_k,λ'_j 是已知数. 由于 $\lambda_{q_m+1}\neq\lambda_{q_m+2}\neq\cdots\neq\lambda_{q_m+p_1}\neq\lambda_{q_m+p_1+1}\neq\lambda_{q_m+p_1+2}\neq\cdots\neq\lambda_{q_m+p_1+p_2}$ 且已知, 因此 $v_{I_{q_m+1}},\ldots,v_{I_{q_m+p_1}}$ 以及 $y_{I_{q_m+1}},\ldots,y_{I_{q_m+p_2}}$ 两两不同且已被固定. 令 $V_0^{p_1}=\{v_{I_{q_m+1}},\ldots,v_{I_{q_m+p_1}}\}$ 以及 $Y_0^{p_2}=\{y_{I_{q_m+1}},\ldots,y_{I_{q_m+p_2}}\}$, 其中 $|V_0^{p_1}|=p_1$ 且 $|Y_0^{p_2}|=p_2$.

由于集合 V^{p_1} 和 Y^{p_2} 有交集, 即 $V^{p_1}\cap Y^{p_2}\neq\emptyset$, 因此我们改进的随机置换模型下的拓展镜像理论不再适用二部图理论, 而是更为通用的图理论.

定义2 (改进的随机置换模型下的拓展镜像理论的图描述)　如果将改进的随机置换模型下的拓展镜像理论中的未知数集合看成是图的顶点, 即顶点集为 $V^{p_1}\cup Y^{p_2}$. 把满足的二变量仿射等式方程看作是图中连接这两个顶点的等边关系, 其值看作是该等边的标签; 把满足的单变量仿射等式方程看作是图的独立顶点 (空边关系), 其值看作是确定的独立顶点标签; 把满足的二变量仿射不等式方程看作是图中连接这两个顶点的不等边关系, 其值看作是该不等边的标签. 于是, 定义 1 描述的拓展镜像系统就可以看成是一个无向带标签图, 记作 $G(\mathcal{E}^{p_1,p_2})=\langle V^{p_1},Y^{p_2},E,L,V_0^{p_1},Y_0^{p_2},L_{V_0^{p_1}},L_{Y_0^{p_2}}\rangle$, 其中

- 顶点集. $V^{p_1}=\{v_1,\dots,v_{q_V^{p_1}}\}$ 和 $Y^{p_2}=\{y_1,\dots,y_{q_Y^{p_2}}\}$ 并且 $|V^{p_1}\cap Y^{p_2}|=\alpha$.
- 边集. $E=E^{=}\cup E^{\neq}$, 其中 $E^{=}=\{e_i=(v_{I_i},y_{I_i})|v_{I_i}\oplus y_{I_i}=\lambda_i,i=1,2,\dots,q_m\}$ 为等边集, $E^{\neq}=\{e'_j=(v_{J_j},y_{J_j})|v_{J_j}\oplus y_{J_j}\neq\lambda'_j,j=1,2,\dots,q_a\}$ 为不等边集.
- 标签函数. $L:E\to\{\lambda_1,\dots,\lambda_{q_m},\lambda'_1,\dots,\lambda'_{q_a}\}$ 是一个标签函数, 对于 $i=1,2,\dots,q_m$ 存在一条边 $e_i\in E^{=}$, 都有 $L(e_i)=\lambda_i$, 对于 $j=1,2,\dots,q_a$, 存在一条边 $e'_j\in E^{\neq}$, 都有 $L(e'_j)\neq\lambda'_j$.
- 独立顶点集. $V_0^{p_1}=\{v_{I_{q_m+1}},\dots,v_{I_{q_m+p_1}}\}$ 和 $Y_0^{p_2}=\{y_{I_{q_m+1}},\dots,y_{I_{q_m+p_2}}\}$.
- 独立顶点标签函数. 对于 $V_0^{p_1}=\{v_{I_{q_m+1}},\dots,v_{I_{q_m+p_1}}\}$ 和 $Y_0^{p_2}=\{y_{I_{q_m+1}},\dots,y_{I_{q_m+p_2}}\}$ 分别有一个一一对应的确定顶点标签, 即 $L_{V_0^{p_1}}=\{\lambda_{q_m+1},\dots,\lambda_{q_m+p_1}\}$ 和 $L_{Y_0^{p_2}}=\{\lambda_{q_m+p_1+1},\dots,\lambda_{q_m+p_1+p_2}\}$.

无向带标签图 $G(\mathcal{E}^{p_1,p_2})=\langle V^{p_1},Y^{p_2},E,L,V_0^{p_1},Y_0^{p_2},L_{V_0^{p_1}},L_{Y_0^{p_2}}\rangle$ 可看成两个子图 $G(\mathcal{E}_m^{p_1,p_2})=\langle V^{p_1},Y^{p_2},E^{=},L,V_0^{p_1},Y_0^{p_2},L_{V_0^{p_1}},L_{Y_0^{p_2}}\rangle$ 和 $G(\mathcal{E}_a)=\langle V^{p_1},Y^{p_2},E^{\neq},L\rangle$ 的叠加, 即 $G(\mathcal{E}^{p_1,p_2})=G(\mathcal{E}_m^{p_1,p_2})\cup G(\mathcal{E}_a)$. 定义路径 $\mathcal{P}$ 的标签为这条路径上所有等边的标签和, 即 $L(\mathcal{P})=\Sigma_{e\in\mathcal{P}}L(e)$.

好的无向带标签图满足的性质. 为确保拓展镜像系统的不重复性和一致性, 即好的无向带标签图应满足如下性质.

- 无圈性. 子图 $G(\mathcal{E}_m^{p_1,p_2})$ 中任意一个连通分支上的任两个顶点 $a,b\in V^{p_1}\cup Y^{p_2}$ 之间只存在一条唯一的路径.
- 连通分支顶点数 $\xi_{\max}$ 有界. 记一个连通分支的大小 (顶点个数) 为 ξ. 在子图 $G(\mathcal{E}_m^{p_1,p_2})$ 中不存在某个连通分支的顶点数大于 $\xi_{\max}$, 即该图的所有连通分支中顶点数最大是 $\xi_{\max}$.
- 不可退化 (非零路径标签). 子图 $G(\mathcal{E}_m^{p_1,p_2})$ 中不存在任何一条偶数长路径 $\mathcal{P}$ 使得 $L(\mathcal{P})=0$.
- 非零圈标签. 定义一个圈 $\mathcal{C}$ 的标签为这条圈上所有边的标签和, 即 $L(\mathcal{C})=\Sigma_{e\in\mathcal{C}}L(e)$. 在图 $G(\mathcal{E}^{p_1,p_2})$ 中不存在包含且仅包含一条不等边的圈 $\mathcal{C}$ 使得 $L(\mathcal{C})=0$.
- 单碰撞顶点. 在 $G(\mathcal{E}_m^{p_1,p_2})$ 每个连通分支中最多包含一个碰撞独立顶点.
- 非零距离标签. 在 $G(\mathcal{E}^{p_1,p_2})$ 中不存在路径距离为 λ' 且选自独立顶点集的两个顶点恰在 λ' 的不等边中.

对于二变量仿射等式方程组, 一旦一个变量被赋值, 则与之连通的连通分支所有元素皆被赋值. 我们的目标就是为 V^{p_1} 以及 Y^{p_2} 集合中的未知数进行赋值, 并计数可能的取值情况.

假设图 $G(\mathcal{E}^{p_1,p_2})$ 可以划分为独立顶点集 $I=V_0^{p_1}\cup Y_0^{p_2}$、$c_1$ 个与 $V_0^{p_1}$ 碰撞的连通分支 $A_1,\dots,A_{c_1}$、c_2 个与 $Y_0^{p_2}$ 碰撞的连通分支 $A_{c_1+1},\dots,A_{c_1+c_2}$、$V^{p_1}\cap Y^{p_2}$ 确定的 α 个边数为 2 且与 I 不碰撞的星型连通分支 $B_1,\dots,B_\alpha$、c_3 个与 $V_0^{p_1}\cup(V^{p_1}\cap Y^{p_2})$ 不碰撞的星型连通分支 $C_1,\dots,C_{c_3}$、c_4 个与 $Y_0^{p_2}\cup(V^{p_1}\cap Y^{p_2})$ 不碰撞的星型连通分支 $C_{c_3+1},\dots,C_{c_3+c_4}$、$c_5$ 个不碰撞的单边连通分支 $D_1,\dots,D_{c_5}$、c_6 个 V^{p_1} 剩余的不等式独立顶点 $E_1,\dots,E_{c_6}$ 以及 c_7 个 Y^{p_2} 剩余的不等式独立顶点 $E_{c_6+1},\dots,E_{c_6+c_7}$, 具体划分方式如图 1 所示.

于是, 有 $G(\mathcal{E}^{p_1,p_2})=I\cup A\cup B\cup C\cup D\cup E$, 其中 I,A,B,C,D,E 分别表示

$$I=V_0^{p_1}\cup Y_0^{p_2},A=A_1\cup\cdots\cup A_{c_1}\cup A_{c_1+1}\cup\cdots\cup A_{c_1+c_2},$$
$$B=B_1\cup\cdots\cup B_\alpha,C=C_1\cup\cdots\cup C_{c_3}\cup C_{c_3+1}\cup\cdots\cup C_{c_3+c_4},$$

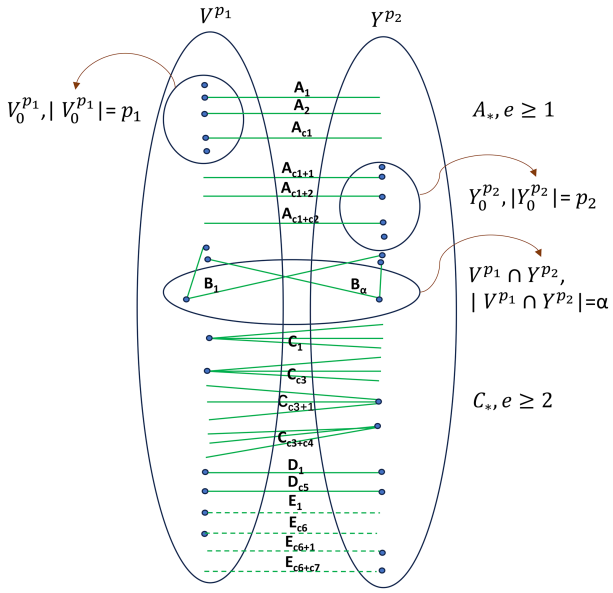

图 1　(网络版彩图) $G(\mathcal{E}^{p_1,p_2})$ **的划分.**

Figure 1　(Color online) Partition of graph $G(\mathcal{E}^{p_1,p_2})$.

$$D = D_1 \cup \cdots \cup D_{c_5}, E = E_1 \cup \cdots \cup E_{c_6} \cup E_{c_6+1} \cup \cdots \cup E_{c_6+c_7}.$$

令 q_1, q_2, q_3, q_4, q_5 分别表示 $A_1 \cup \cdots \cup A_{c_1}$, $A_{c_1+1} \cup \cdots \cup A_{c_1+c_2}$, $C_1 \cup \cdots \cup C_{c_3}$, $C_{c_3+1} \cup \cdots \cup C_{c_3+c_4}$ 以及 $D_1 \cup \cdots \cup D_{c_5}$ 的等边数 (等式的数量). 于是, 我们得到了定理 1.

定理1 (改进的拓展镜像理论下界)　令 $G(\mathcal{E}^{p_1,p_2}) = \langle V^{p_1}, Y^{p_2}, E, L, V_0^{p_1}, Y_0^{p_2}, L_{V_0^{p_1}}, L_{Y_0^{p_2}} \rangle$ 是由改进的随机置换模型下的拓展镜像系统导出的无向带标签图, $|V^{p_1} \cap Y^{p_2}| = \alpha \leqslant q_m/2^{n/3}$ 且 $G(\mathcal{E}^{p_1,p_2}) = I \cup A \cup B \cup C \cup D \cup E$. 令 $q' = q_2 + \alpha + c_3 + q_4 + q_5 + c_6$ 和 $q'' = q_1 + \alpha + q_3 + c_4 + q_5 + c_7$. 令 η_i 表示第 i 个连通分支的边数, 其中 $1 \leqslant i \leqslant c_1 + c_2 + \alpha + c_3 + c_4 + c_5$.

(1) 对于带有不等式约束的强 (可调) 伪随机置换假设下, 选自 $\{0,1\}^n$ 且满足镜像系统 $G(\mathcal{E}^{p_1,p_2})$ 的所有可能解的个数至少为

$$\frac{(2^n - p_1)_{q'}(2^n - p_2)_{q''}}{\prod_{\lambda \in \lambda^{*q_m}} (2^n)_{\mu(\lambda^{*q_m}, \lambda)}} \left(1 - \frac{2(p_1+q_m)^2 \sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1} \eta_{i+1}^2 + 2(p_2+q_m)^2 \sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1} \eta_{i+1}^2}{2^{2n}}\right.$$
$$- \frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1} \eta_{i+1} + c_5)}{2^{2n}} - \frac{19q_m}{2^{2n/3}} - \frac{16(p_1+p_2+q_m)}{q_m 2^{n/3}}$$
$$\left. - \frac{2(c_3+c_4+c_5)q_m^2}{2^{2n}} - \frac{\sum_{i=1}^{c_1+c_2} q_m}{2^n} - \frac{2q_m}{2^n} - \frac{2q_a}{2^n}\right).$$

(2) 对于带有不等式约束的 (可调) 伪随机函数或消息认证码假设下, 选自 $\{0,1\}^n$ 且满足镜像系统 $G(\mathcal{E}^{p_1,p_2})$ 的所有可能解的个数至少为

$$\frac{(2^n - p_1)_{q'}(2^n - p_2)_{q''}}{2^{nq_m}} \left(1 - \frac{2(p_1+q_m)^2 \sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1} \eta_{i+1}^2 + 2(p_2+q_m)^2 \sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1} \eta_{i+1}^2}{2^{2n}}\right.$$
$$\left. - \frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1} \eta_{i+1} + c_5)}{2^{2n}} - \frac{19q_m}{2^{2n/3}} - \frac{16(p_1+p_2+q_m)}{q_m 2^{n/3}} - \frac{2q_a}{2^n}\right).$$

证明　令 $h(G)$ 表示镜像系统 $G(\mathcal{E}^{p_1,p_2})$ 的解的个数. 我们计算 $h(G)$ 的计数策略是: 先进行独立顶点集的赋值 (实际上已经被固定了, 也就是说后续计数时需要排除掉这些固定好的值), 然后依次进

行 A, B, C, D, E 赋值, 计算所有可能的计数. 在对 I, A, B, C, D, E 计数之前, 我们先给出一些公共知识.

对于第 i 个连通分支, 令 ξ_i 表示其顶点个数 (大小), η_i 表示其边数, 其中 $1 \leqslant i \leqslant c_1 + c_2 + c_3 + c_4 + c_5 + \alpha$. 对于每个 $1 \leqslant j \leqslant \eta_i$ 以及 $r = \sum_{k=1}^{i-1} \eta_k + j$, 有

- $\lambda^r = \lambda_i^j$ 即第 i 个连通分支的第 j 个等式方程的标签;
- 对于强 (可调) 伪随机置换设置, $\delta_i^j = \mu(\lambda^{r-1}, \lambda_i^j)$ 且 $\delta_1^1 = 0$;
- 对于 (可调) 伪随机函数或消息认证码设置, $\delta_i^j = 0$.

当第 i 个连通分支只包含一条边时, 则可以去掉上标, 即 λ_i^j, δ_i^j 退化成 λ_i, δ_i.

假设第 i 个连通分支中来自于 V^{p_1} 的顶点集合为 V_i, 来自于 Y^{p_2} 的顶点集合为 Y_i, 那么对于非 B 的集合都有 $\xi_i = |V_i| + |Y_i|$. 令 v_i^j 表示 V_i 的第 j 个顶点, y_i^j 表示 Y_i 的第 j 个顶点. 当 V_i 或 Y_i 只包含一个顶点时, 去掉上标, 即 v_i^j, y_i^j 退化成 v_i, y_i. 令 a_i^v 表示第 i 个连通分支中顶点与以前连通分支中 v 顶点相连的不等边的条数. 令 a_i^y 表示第 i 个连通分支中顶点与以前连通分支中 y 顶点相连的不等边的条数. 令 $a_i = a_i^v + a_i^y$ 并且 $c = c_1 + c_2 + c_3 + c_4 + c_5 + \alpha$, 则 $q_a = \sum_{i=1}^{c+c_6+c_7} a_i$.

首先, 对独立顶点集 $I = V_0^{p_1} \cup Y_0^{p_2}$ 进行赋值计数. 根据单变量方程组系统, 这个独立顶点集实际上已经被固定了. 后续对顶点集计数需要从取值空间中去掉这些确定的独立顶点, 即考虑 $V^{p_1} \setminus V_0^{p_1}$ 以及 $Y^{p_2} \setminus Y_0^{p_2}$.

然后, 在独立顶点集 $I = V_0^{p_1} \cup Y_0^{p_2}$ 选好的情况下, 选择 A 中所有顶点进行计数. 令 $h(c_1 + c_2)$ 表示镜像系统 $I \cup A$ 的解的个数. 子图 A 是由 c_1 个与 $V_0^{p_1}$ 碰撞的连通分支 $A_1, \ldots, A_{c_1}$ 以及 c_2 个与 $Y_0^{p_2}$ 碰撞的连通分支 $A_{c_1+1}, \ldots, A_{c_1+c_2}$ 组成. 在子图 A 中, 由于 $I = V_0^{p_1} \cup Y_0^{p_2}$ 均已选好, 因此子图 A 元素均已固定, 也就是说 $h(c_1 + c_2) = 1$.

根据 q_1 和 q_2 分别表示连通分支 $A_1, \ldots, A_{c_1}$ 和 $A_{c_1+1}, \ldots, A_{c_1+c_2}$ 的等边数 (等式的数量). 于是, 根据 $\sum_{i=1}^{c_1+c_2} \eta_i = q_1 + q_2$ 以及 $\sum_{j=1}^{\eta_i} \delta_i^j \leqslant \delta$ (对于强 (可调) 伪随机置换设置下, $\delta \leqslant q_m$; 对于 (可调) 伪随机函数或消息认证码设置下, $\delta = 0$), 有

$$\begin{aligned}
&\frac{h(c_1+c_2)\prod_{i=1}^{c_1+c_2}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}{(2^n-p_1)_{q_2}(2^n-p_2)_{q_1}} \geqslant \frac{\prod_{i=1}^{c_1+c_2}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}{(2^n)^{q_1+q_2}} \\
&\geqslant \frac{(2^n)^{\sum_{i=1}^{c_1+c_2}\eta_i} - (2^n)^{\sum_{i=1}^{c_1+c_2}\eta_i - 1}\sum_{i=1}^{c_1+c_2}\sum_{j=1}^{\eta_i} 2^n\delta_i^j}{(2^n)^{q_1+q_2}} \geqslant 1 - \frac{\sum_{i=1}^{c_1+c_2}\sum_{j=1}^{\eta_i}\delta_i^j}{2^n} \geqslant 1 - \frac{\sum_{i=1}^{c_1+c_2}\delta}{2^n}.
\end{aligned}$$

令新的顶点集为

$$V_i = \bigcup_{j=c_1+1}^{c_1+c_2} V_j \cup \bigcup_{k=c_1+c_2+1}^{i} V_k, \quad Y_i = \bigcup_{j=1}^{c_1} Y_j \cup \bigcup_{k=c_1+c_2+1}^{i} Y_k.$$

在独立顶点集 I 和子图 A 选好的基础上, 对于子图 B, 计算 $I \cup A \cup B$ 的所有可能计数. 子图 B 是由 $V^{p_1} \cap Y^{p_2}$ 确定的 α 个边数为 2 且与 $I \cup \bigcup_{j=1}^{c_1} Y_j \cup \bigcup_{j=c_1+1}^{c_1+c_2} V_j$ 不碰撞的星型连通分支 $B_1, \ldots, B_\alpha$ 组成. 根据 $|V^{p_1} \cap Y^{p_2}| = \alpha$, 定义一个无序集合 S 如下:

$$S = \{(v_1, y_1), (v_1', y_1'), \ldots, (v_\alpha, y_\alpha), (v_\alpha', y_\alpha')\}$$

使得对于 $1 \leqslant i \leqslant \alpha$ 都有 $v_i = y_i'$. 如果无序集合 S 满足如下条件, 则称为良好可选集.

- 对于 $1 \leqslant i \leqslant \alpha$, $(v_1, y_1), (v_1', y_1'), \ldots, (v_\alpha, y_\alpha), (v_\alpha', y_\alpha')$ 两两不同;
- 对于 $1 \leqslant i \leqslant \alpha$, $v_i' \oplus y_i \notin V_0^{p_1} \cup V_i$ 且两两不同;
- 对于 $1 \leqslant i \leqslant \alpha$, $v_i' \oplus y_i \notin Y_0^{p_2} \cup Y_i$ 且两两不同.

实际上, 子图 B 是从 $s = q_m - q_1 - q_2$ 个 (v, y) 选出的 α 个具有良好可选集的计数. 这里假设 $1 \leqslant \alpha \leqslant M = q_m/2^{n/3}$ 并令 $N_S(\alpha)$ 为子图 B 的所有可能计数. 这里采用逐步构建良好可选集 S, 先

从 (v_1,y_1), (v_1',y_1') 开始, 共有 $s(s-1)-(p_1+q_2+p_2+q_1)$ 种选择; 然后是 (v_2,y_2), (v_2',y_2'), 考虑上面的条件, 共有 $(s-2)(s-5)-(p_1+q_2+p_2+q_1)$; 直到最后 (v_α,y_α), (v_α',y_α'), 考虑上面的条件, 共有 $(s-2\alpha+2)(s-4\alpha+3)-(p_1+q_2+p_2+q_1)$. 于是, 根据 $s-2M-q_1-q_2\geqslant s/2$, 有

$$\begin{aligned}
N_S(\alpha)\geqslant&\frac{1}{\alpha!}\prod_{l=0}^{\alpha-1}((s-2l)(s-4l-1)-(p_1+q_2+p_2+q_1))\\
=&\frac{(s)_{2\alpha}}{\alpha!}\prod_{l=0}^{\alpha-1}\frac{(s-2l)(s-4l-1)-(p_1+q_2+p_2+q_1)}{(s-2l)(s-2l-1)}\\
\geqslant&\frac{(s)_{2\alpha}}{\alpha!}\prod_{l=0}^{\alpha-1}\left(1-\frac{2ls+p_1+q_2+p_2+q_1}{(s-2l)(s-2l-1)}\right)\geqslant\frac{(s)_{2\alpha}}{\alpha!}\left(1-\sum_{l=0}^{\alpha-1}\frac{2ls+p_1+q_2+p_2+q_1}{(s-2M)^2}\right)\\
\geqslant&\frac{(s)_{2\alpha}}{\alpha!}\left(1-\frac{4s\alpha^2+4(p_1+q_2+p_2+q_1)\alpha}{s^2}\right)\geqslant\frac{(s)_{2\alpha}}{\alpha!}\left(1-\frac{4sM^2+4(p_1+q_2+p_2+q_1)M}{s^2}\right)\\
\geqslant&\frac{(s)_{2\alpha}}{\alpha!}\left(1-\frac{8q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}\right).
\end{aligned}$$

于是, 我们有

$$\begin{aligned}
&\sum_{\alpha=1}^{M}\frac{N_S(\alpha)\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha(2^n-p_2-q_1)_\alpha}\\
&\geqslant\sum_{\alpha=1}^{M}\frac{(s)_{2\alpha}}{\alpha!}\left(1-\frac{8q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}\right)\frac{\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha(2^n-p_2-q_1)_\alpha}\\
&=\left(1-\frac{8q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}\right)\cdot\sum_{\alpha=1}^{M}\underbrace{\frac{(s)_{2\alpha}}{(s)_\alpha(s)_\alpha}}_{A_1}\cdot\underbrace{\frac{(s)_\alpha(s)_\alpha}{\alpha!}\cdot\frac{\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha(2^n-p_2-q_1)_\alpha}}_{A_2}.
\end{aligned}$$

对于 A_1, 根据 $1\leqslant\alpha\leqslant M=q_m/2^{n/3}$ 以及 $s=q_m-q_1-q_2\geqslant q_m/2$, 有

$$A_1=\frac{(s)_{2\alpha}}{(s)_\alpha(s)_\alpha}\geqslant\frac{(s)_{2\alpha}}{(s)^{2\alpha}}=\prod_{i=0}^{2\alpha-1}\left(1-\frac{i}{s}\right)\geqslant1-\sum_{i=0}^{2\alpha-1}\frac{i}{s}=1-\frac{4\alpha^2}{s}\geqslant1-\frac{8q_m}{2^{2n/3}}.$$

对于 A_2, 根据 $1\leqslant\alpha\leqslant M=q_m/2^{n/3}$, $2^n-p_1-q_2-p_2-q_1-2M\geqslant2^n/2$ 以及 $\sum_{i=1}^{\alpha}\delta_i=\delta$, 有

$$\begin{aligned}
A_2=&\frac{(s)_\alpha(s)_\alpha}{\alpha!}\cdot\frac{\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha\cdot(2^n-p_2-q_1)_\alpha}\\
=&\underbrace{\frac{(s)_\alpha(s)_\alpha}{\alpha!}\cdot\frac{(2^n-s)_{s-\alpha}}{(2^n)_s}}_{\mathrm{HYP}_{2^n,s,s}(\alpha)}\cdot\frac{(2^n)_s\cdot\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-s)_{s-\alpha}\cdot(2^n-p_1-q_2)_\alpha\cdot(2^n-p_2-q_1)_\alpha}\\
=&\mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\underbrace{\frac{(2^n)_{s-\alpha}}{(2^n-s)_{s-\alpha}}}_{\geqslant1}\cdot\frac{(2^n-s+\alpha)_\alpha}{(2^n-p_1-q_2)_\alpha}\cdot\frac{\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_2-q_1)_\alpha}\\
\geqslant&\mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\prod_{i=0}^{\alpha-1}\frac{2^n-s+\alpha-i}{2^n-p_1-q_2-i}\cdot\prod_{i=1}^{\alpha}\frac{2^n-\delta_i}{2^n-p_2-q_1-i+1}\\
\geqslant&\mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\prod_{i=0}^{\alpha-1}\left(1-\frac{s}{2^n-p_1-q_2-i}\right)\cdot\prod_{i=1}^{\alpha}\left(1-\frac{\delta_i}{2^n-p_2-q_1-i+1}\right)\\
\geqslant&\mathrm{HYP}_{2^n,s,s(\alpha)}\cdot\left(1-\sum_{i=0}^{\alpha-1}\frac{s}{2^n-p_1-q_2-i}\right)\cdot\left(1-\sum_{i=1}^{\alpha}\frac{\delta_i}{2^n-p_2-q_1-i+1}\right)
\end{aligned}$$

$$\geqslant \mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\left(1-\frac{2s\alpha}{2^n}\right)\cdot\left(1-\frac{2\delta}{2^n}\right)\geqslant \mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\left(1-\frac{2sM}{2^n}\right)\cdot\left(1-\frac{2\delta}{2^n}\right)$$
$$\geqslant \mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\left(1-\frac{2q_m^2}{2^{4n/3}}\right)\cdot\left(1-\frac{2\delta}{2^n}\right)\geqslant \mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\left(1-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right).$$

于是, 根据 $\frac{q_m^2}{2^{4n/3}}\leqslant\frac{q_m}{2^{2n/3}}$ 以及 $s=q_m-q_1-q_2\geqslant q_m/2$, 有

$$\begin{aligned}
&\sum_{\alpha=1}^{M}\frac{N_S(\alpha)\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha(2^n-p_2-q_1)_\alpha}\\
&\geqslant\left(1-\frac{8q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}\right)\cdot\sum_{\alpha=1}^{M}\left(1-\frac{8q_m}{2^{2n/3}}\right)\cdot\mathrm{HYP}_{2^n,s,s}(\alpha)\cdot\left(1-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right)\\
&=\left(1-\frac{8q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}\right)\cdot\left(1-\frac{8q_m}{2^{2n/3}}\right)\cdot\left(1-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right)\cdot\sum_{\alpha=1}^{M}\mathrm{HYP}_{2^n,s,s}(\alpha)\\
&\geqslant\left(1-\frac{16q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right)\cdot\sum_{\alpha=1}^{M}\mathrm{HYP}_{2^n,s,s}(\alpha)\\
&=\left(1-\frac{16q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right)\cdot\left(1-\sum_{\alpha\geqslant M}\mathrm{HYP}_{2^n,s,s}(\alpha)\right)\\
&\geqslant\left(1-\frac{16q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}-\frac{2q_m^2}{2^{4n/3}}-\frac{2\delta}{2^n}\right)\cdot\left(1-\frac{E[\mathrm{HYP}_{2^n,s,s}(\alpha)]}{M}\right)\\
&\geqslant\left(1-\frac{18q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}-\frac{2\delta}{2^n}\right)\cdot\left(1-\frac{s^2/2^n}{M}\right)\\
&\geqslant 1-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{n/3}}-\frac{2\delta}{2^n}.
\end{aligned}$$

接着, 在独立顶点集 I 和子图 $A\cup B$ 选好的基础上, 对于子图 C, 计算 $I\cup A\cup B\cup C$ 的所有可能计数. 子图 C 是由 c_3 个与 $V_0^{p_1}\cup\bigcup_{j=c_1+1}^{c_1+c_2+\alpha}V_j$ 不碰撞的星型连通分支 $C_1,\ldots,C_{c_3}$ 以及 c_4 个与 $Y_0^{p_2}\cup\bigcup_{j=1}^{c_1}Y_j\bigcup_{j=c_1+c_2+1}^{c_1+c_2+\alpha}Y_j$ 不碰撞的星型连通分支 $C_{c_3+1},\ldots,C_{c_3+c_4}$ 组成. 对于 $i=1,\ldots,c_3+c_4$ 以及 $i'=c_1+c_2+\alpha+i$, 令 $h_C(i)=h(i')$ 表示 $I\cup A\cup B\cup C_1\cup\cdots\cup C_i$ 的所有可能计数. 初始条件 $h_C(0)=h(c_1+c_2+\alpha)$, 目标是给出 $\frac{h_C(i+1)}{h_C(i)}$ 的递推表达式, 从而得到最后的 $h_C(c_3+c_4)=h(c_1+c_2+\alpha+c_3+c_4)$. 考虑到对星型连通分支 $C_1,\ldots,C_{c_3}$ 以及星型连通分支 $C_{c_3+1},\ldots,C_{c_3+c_4}$ 的分析类似性, 我们详细介绍对星型连通分支 $C_1,\ldots,C_{c_3}$ 的分析过程. 如果我们分配给 $V_{i'+1}$ 中某个元素 $v_{i'+1}$ 一个值, 那么根据第 $i'+1$ 个连通分支, 与之连通的 $\eta_{i'+1}$ 个未知数将被唯一确定. 那么 $h_C(i+1)$ 就是 $V_0^{p_1}\cup V_{i'}\cup\{v_{i'+1}\}\cup Y_0^{p_2}\cup Y_{i'}\cup\{y_{i'+1}^1,\ldots,y_{i'+1}^{\eta_{i'+1}}\}$ 的赋值计数, 并且满足如下条件:

(1) $V_0^{p_1}\cup V_{i'}\cup Y_0^{p_2}\cup Y_{i'}$ 满足 $h_B(i)$;

(2) 对于 $j=1,\ldots,\eta_{i'+1}$ 满足 $v_{i'+1}\oplus y_{i'+1}^j=\lambda_{i'+1}^j$;

(3) $v_{i'+1}\notin V_0^{p_1}\cup V_{i'}$;

(4) 对于 $j=1,\ldots,\eta_{i'+1}$ 满足 $y_{i'+1}^j\notin Y_0^{p_2}\cup Y_{i'}$ 并且后续赋值均不与以前赋值重复;

(5) $v_{i'+1}$ 满足 $a_{i'+1}^v$ 个与以前连通分支中 Y^{p_2} 相连的不等式;

(6) 对于 $j=1,\ldots,\eta_{i'+1}$, 有 $y_{i'+1}^j$ 满足 $a_{i'+1}^y$ 个与以前连通分支中 V^{p_1} 相连的不等式.

如果只满足条件 (1) 和 (2), 则有 $2^nh_C(i)$ 可能的计数, 而条件 (3) 排除了 $|V_0^{p_1}\cup V_{i'}|=p_1+|V_{i'}|$ 个可能的计数, 条件 (4) 排除了 $\eta_{i'+1}|Y_0^{p_2}\cup Y_{i'}|=\eta_{i'+1}(p_2+|Y_{i'}|)$ 个可能的计数. 除此之外, 还有 $\sum_{j=1}^{\eta_{i'+1}}\delta_{i'+1}^j$ 以前的等式与 C_{i+1} 中等式贡献相同的 λ. 条件 (5) 排除了 $a_{i'+1}^v$ 个可能的计数, 条件 (6)

排除了 $a^y_{i'+1}$ 个可能的计数. 因此, 有

$$h_C(i+1)\geqslant\left(2^n-(p_1+|V_{i'}|)-\eta_{i'+1}(p_2+|Y_{i'}|)-a^v_{i'+1}-a^y_{i'+1}+\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1}\right)h_C(i).$$

进一步地, 对于 $i=1,\dots,c_3-1$ 以及 $i'=c_1+c_2+i$, 根据 $a^v_{i'+1}+a^y_{i'+1}=a_{i'+1}$, $|V_{i'}|\leqslant q_m$, $|Y_{i'}|\leqslant q_m, p_1+|V_{i'}|\leqslant 2^{n-1}$, $p_2+|Y_{i'}|\leqslant 2^{n-1}$ 以及 $\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1}=\delta$, 有

$$\begin{aligned}
&\frac{h_C(i+1)\prod_{j=1}^{\eta_{i'+1}}(2^n-\delta^j_{i'+1})}{h_C(i)(2^n-(p_1+|V_{i'}|))(2^n-(p_2+|Y_{i'}|))_{\eta_{i'+1}}}\\
\geqslant&\frac{(2^n-(p_1+|V_{i'}|)-\eta_{i'+1}(p_2+|Y_{i'}|)-a^v_{i'+1}-a^y_{i'+1}+\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1})\prod_{j=1}^{\eta_{i'+1}}(2^n-\delta^j_{i'+1})}{(2^n-(p_1+|V_{i'}|))\,(2^n-(p_2+|Y_{i'}|))_{\eta_{i'+1}}}\\
\geqslant&1-\frac{\eta^2_{i'+1}(p_1+|V_{i'}|)^2(2^n)^{\eta_{i'+1}-1}+\eta_{i'+1}(p_1+|V_{i'}|)(p_2+|Y_{i'}|)(2^n)^{\eta_{i'+1}-1}}{(2^n-(p_1+|V_{i'}|))\,(2^n-(p_2+|Y_{i'}|))_{\eta_{i'+1}}}\\
&-\frac{a_{i'+1}(2^n)^{\eta_{i'+1}}+(\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1})^2(2^n)^{\eta_{i'+1}-1}}{(2^n-(p_1+|V_{i'}|))\,(2^n-(p_2+|Y_{i'}|))_{\eta_{i'+1}}}\\
\geqslant&1-\frac{\eta^2_{i'+1}(p_1+q_m)^2(2^n)^{\eta_{i'+1}-1}+\eta_{i'+1}(p_1+q_m)(p_2+q_m)(2^n)^{\eta_{i'+1}-1}}{(2^n)^{\eta_{i'+1}+1}/2}\\
&-\frac{a_{i'+1}(2^n)^{\eta_{i'+1}}+(\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1})^2(2^n)^{\eta_{i'+1}-1}}{(2^n)^{\eta_{i'+1}+1}/2}\\
\geqslant&1-\frac{2\eta^2_{i'+1}(p_1+q_m)^2+2\eta_{i'+1}(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i'+1}}{2^n}.
\end{aligned}$$

类似地, 对于星型连通分支 $C_{c_3+1},\dots,C_{c_3+c_4}$ 也有相似结果. 具体来说, 对于 $i=1,\dots,c_4-1$ 以及 $i'=c_1+c_2+\alpha+c_3+i$, 根据 $a^v_{i'+1}+a^y_{i'+1}=a_{i'+1}$, $|V_{i'}|\leqslant q_m$, $|Y_{i'}|\leqslant q_m, \xi_{\max}(p_1+|V_{i'}|+p_2+|Y_{i'}|)\leqslant 2^{n-1}$ 以及 $\sum_{j=1}^{\eta_{i'+1}}\delta^j_{i'+1}=\delta$, 我们有

$$\begin{aligned}
&\frac{h_C(i+1)\prod_{j=1}^{\eta_{i'+1}}(2^n-\delta^j_{i'+1})}{h_C(i)(2^n-(p_1+|V_{i'}|))_{\eta_{i'+1}}(2^n-(p_2+|Y_{i'}|))}\\
&\geqslant 1-\frac{2\eta^2_{i'+1}(p_2+q_m)^2+2\eta_{i'+1}(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i'+1}}{2^n}.
\end{aligned}$$

于是, 在独立顶点集 I 和子图 $A\cup B$ 选好的基础上, 对于子图 C, 计算 $I\cup A\cup B\cup C$ 的所有可能计数为

$$\begin{aligned}
&\frac{h_C(c_3+c_4)\prod_{i=c_1+c_2+\alpha+1}^{c_1+c_2+\alpha+c_3+c_4}\prod_{j=1}^{\eta_i}(2^n-\delta^j_i)}{(2^n-p_1-q_2-\alpha)_{c_3+q_4}(2^n-p_2-q_1-\alpha)_{q_3+c_4}}\\
\geqslant&\prod_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}\left(1-\frac{2\eta^2_{i+1}(p_1+q_m)^2+2\eta_{i+1}(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i+1}}{2^n}\right)\\
&\cdot\prod_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}\left(1-\frac{2\eta^2_{i+1}(p_2+q_m)^2+2\eta_{i+1}(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i+1}}{2^n}\right)\\
\geqslant&1-\frac{\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}2\eta^2_{i+1}(p_1+q_m)^2+\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}2\eta_{i+1}(p_1+q_m)(p_2+q_m)+2(c_3+c_4)\delta^2}{2^{2n}}\\
&-\frac{\sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}2\eta^2_{i+1}(p_2+q_m)^2}{2^{2n}}-\frac{2\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}a_{i+1}}{2^n}.
\end{aligned}$$

接着, 在独立顶点集 I、子图 A 和子图 $B\cup C$ 选好的基础上, 对于子图 D, 计算 $I\cup A\cup B\cup C\cup D$ 的所有可能计数. 子图 D 是由 c_5 个单边连通分支 $D_1,\dots,D_{c_5}$ 组成. 令 $c'=c_1+c_2+\alpha+c_3+c_4$.

对于 $i=1,\dots,c_5$ 以及 $i''=c_1+c_2+\alpha+c_3+c_4+i=c'+i$, 单边连通分支 $D_i: v_{i''}\oplus y_{i''}=\lambda_{i''}$, 其中 $v_{i''}\in V_{i''}$, $y_{i''}\in Y_{i''}$. 令 $h_D(i)=h(i')$ 表示 $I\cup A\cup\cup B\cup C\cup D_1\cup\cdots\cup D_i$ 的所有可能计数. 初始条件 $h_D(0)=h(c_1+c_2+\alpha+c_3+c_4)$, 目标是给出 $\frac{h_D(i+1)}{h_D(i)}$ 的递推表达式, 从而得到最后的 $h_D(c_5)=h(c_1+c_2+\alpha+c_3+c_4+c_5)$. 一旦前 i 个单边连通分支的顶点被选好之后, 第 $i+1$ 个单边连通分支的计数 $h_D(i+1)$ 就是 $V_0^{p_1}\cup V_{c'}\cup\{v_{c'+1},\dots,v_{i''+1}\}\cup Y_0^{p_2}\cup Y_{c'}\cup\{y_{c'+1},\dots,y_{i''+1}\}$ 的赋值计数, 并且满足如下条件:

(1) $V_0^{p_1}\cup V_{c'}\cup\{v_{c'+1},\dots,v_{i''}\}\cup Y_0^{p_2}\cup Y_{c'}\cup\{y_{c'+1},\dots,y_{i''}\}$ 满足 $h_C(i)$;

(2) $v_{i''+1}\oplus y^j_{i''+1}=\lambda^j_{i''+1}$;

(3) $v_{i''+1}\notin V_0^{p_1}\cup V_{c'}\cup\{v_{c'+1},\dots,v_{i''}\}$;

(4) $y_{i''+1}\notin Y_0^{p_2}\cup Y_{c'}\cup\{y_{c'+1},\dots,y_{i''}\}$;

(5) $v_{i''+1}$ 满足 $a^v_{i''+1}$ 个与以前连通分支中 Y^{p_2} 相连的不等式;

(6) $y_{i''+1}$ 满足 $a^y_{i''+1}$ 个与以前连通分支中 V^{p_1} 相连的不等式.

如果只满足条件 (1) 和 (2), 则有 $2^n h_D(i)$ 可能的计数, 而条件 (3) 排除了 $|V_0^{p_1}\cup V_{c'}\cup\{v_{c'+1},\dots,v_{i''}\}|=p_1+|V_{c'}|+i$ 个可能的计数, 条件 (4) 排除了 $|Y_0^{p_2}\cup Y_{c'}\cup\{y_{c'+1},\dots,y_{i''}\}|=p_2+|Y_{c'}|+i$ 个可能的计数. 除此之外, 还有 $\delta_{i''+1}$ 以前的等式与 C_{i+1} 中等式贡献相同的 λ. 条件 (5) 排除了 $a^v_{i''+1}$ 个可能的计数, 条件 (6) 排除了 $a^y_{i''+1}$ 个可能的计数. 因此, 有

$$h_D(i+1)\geqslant\left(2^n-(p_1+|V_{c'}|+i)-(p_2+|Y_{c'}|+i)-a^v_{i''+1}-a^y_{i''+1}+\delta_{i''+1}\right)h_D(i).$$

进一步地, 对于 $i=1,\dots,c_5-1$ 以及 $i''=c'+i$, 根据 $a^v_{i''+1}+a^y_{i''+1}=a_{i''+1}$, $|V_{c'}|+i\leqslant q_m$, $|Y_{c'}|+i\leqslant q_m, p_1+|V_{c'}|+i+p_2+|Y_{c'}|+i\leqslant 2^{n-1}$ 以及 $\delta_{i''+1}=\delta$, 有

$$\begin{aligned}
&\frac{h_D(i+1)(2^n-\delta_{i''+1})}{h_D(i)(2^n-(p_1+|V_{c'}|+i))(2^n-(p_2+|Y_{c'}|+i))}\\
&\geqslant\frac{(2^n-(p_1+|V_{c'}|+i)-(p_2+|Y_{c'}|+i)-a^v_{i''+1}-a^y_{i''+1}+\delta_{i''+1})(2^n-\delta_{i''+1})}{(2^n-(p_1+|V_{c'}|+i))(2^n-(p_2+|Y_{c'}|+i))}\\
&\geqslant 1-\frac{(p_1+|V_{c'}|+i)(p_2+|Y_{c'}|+i)+2^n a_{i''+1}+\delta^2_{i''+1}}{(2^n-(p_1+|V_{c'}|+i))(2^n-(p_2+|Y_{c'}|+i))}\\
&\geqslant 1-\frac{(p_1+q_m)(p_2+q_m)+2^n a_{i''+1}+\delta^2_{i''+1}}{2^{2n}/2}\\
&\geqslant 1-\frac{2(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i''+1}}{2^n}.
\end{aligned}$$

于是, 在独立顶点集 I、子图 A 以及子图 $B\cup C$ 选好的基础上, 对于子图 D, 计算 $I\cup A\cup B\cup C\cup D$ 的所有可能计数为

$$\begin{aligned}
&\frac{h_D(c_5)\prod_{i''=c'+1}^{c'+c_5}(2^n-\delta_i)}{(2^n-p_1-q_2-\alpha-c_3-q_4)_{q_5}(2^n-p_2-q_1-\alpha-q_3-c_4)_{q_5}}\\
&\geqslant\prod_{i''=c'+1}^{c'+c_5}\left(1-\frac{2(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}-\frac{2a_{i''+1}}{2^n}\right)\\
&\geqslant 1-\sum_{i''=c'+1}^{c'+c_5}\left(\frac{2(p_1+q_m)(p_2+q_m)+2\delta^2}{2^{2n}}+\frac{2a_{i''+1}}{2^n}\right)\\
&\geqslant 1-\frac{2c_5(p_1+q_m)(p_2+q_m)+2c_5\delta^2}{2^{2n}}-\frac{2\sum_{i''=c'+1}^{c'+c_5}a_{i''+1}}{2^n}.
\end{aligned}$$

最后, 我们对不在等式方程组中的不等式方程组系统图顶点进行赋值计数. 在独立顶点集 I、子图 $A\cup B$ 以及子图 $C\cup D$ 选好的基础上, 对于子图 E, 计算 $I\cup A\cup B\cup C\cup D\cup E$ 的所有可能计数. 子

图 E 是由 c_6 个 V^{p_1} 剩余独立顶点 $E_1,\dots,E_{c_6}$ 以及 c_7 个 $Y_0^{p_2}$ 剩余独立顶点 $E_{c_6+1},\dots,E_{c_6+c_7}$ 不等式独立顶点集组成. 令 $c=c_1+c_2+\alpha+c_3+c_4+c_5$, 对于 $i=1,\dots,c_6+c_7$ 以及 $i'=c+i$, 令 $h_E(i)$ 表示 $I\cup A\cup B\cup C\cup D\cup E_1\cup\cdots\cup E_i$ 的所有可能计数. 初始条件 $h_E(0)=h_D(c_5)$, 目标是给出 $\frac{h_E(i+1)}{h_E(i)}$ 的递推表达式, 从而得到最后的 $h_E(c_6+c_7)$. 对于 $E_1\cup\cdots\cup E_{c_6}$, $h_E(i+1)$ 就是 $V_0^{p_1}\cup V_c\cup\{v_{c+1},\dots,v_{i'+1}\}$ 的赋值计数, 并且满足如下条件:

(1) $V_0^{p_1}\cup V_c\cup\{v_{c+1},\dots,v_{i'}\}$ 满足 $h_E(i)$;

(2) $v_{i'+1}\notin V_0^{p_1}\cup V_c\cup\{v_{c+1},\dots,v_{i'}\}$;

(3) $v_{i'+1}$ 满足 $a^v_{i'+1}$ 个与以前连通分支中 Y^{p_2} 相连的不等式.

如果只满足条件 (1), 则有 $2^nh_E(i)$ 可能的计数, 而条件 (2) 排除了 $|V_0^{p_1}\cup V_c\cup\{v_{c+1},\dots,v_{i'}\}|=p_1+|V_c|+i$ 个可能的计数, 条件 (3) 排除了 $a^v_{i'+1}$ 个可能的计数. 因此, 有

$$h_E(i+1)\geqslant\left(2^n-(p_1+|V_c|+i)-a^v_{i'+1}\right)h_E(i).$$

进一步地, 根据 $|V_c|+i\leqslant q_m$, $|Y_c|+i\leqslant q_m$, $p_1+|V_c|+i\leqslant 2^{n-1}$, $p_2+|Y_c|+i\leqslant 2^{n-1}$, 有

$$\begin{aligned}&\frac{h_E(i+1)}{h_E(i)(2^n-p_1-q_2-\alpha-c_3-q_4-q_5)_{c_6}}\geqslant\prod_{i=0}^{c_6-1}\frac{2^n-(p_1+|V_c|+i)-a^v_{i'+1}}{2^n-p_1-q_2-\alpha-c_3-q_4-q_5-i}\\&\geqslant 1-\sum_{i=0}^{c_6-1}\frac{a^v_{i'+1}}{2^n-p_1-q_2-\alpha-c_3-q_4-q_5-i}\geqslant 1-\frac{2\sum_{i'=c}^{c+c_6-1}a^v_{i'+1}}{2^n}.\end{aligned}$$

类似于, 对于 $E_{c_6+1}\cup\cdots\cup E_{c_6+c_7}$, 也有相似结果. 因此综合考虑 E, 有

$$\begin{aligned}&\frac{h_E(c_6+c_7)}{(2^n-p_1-q_2-\alpha-c_3-q_4-q_5)_{c_6}(2^n-p_2-q_1-\alpha-q_3-c_4-q_5)_{c_7}}\\&\geqslant\left(1-\frac{2\sum_{i'=c}^{c+c_6-1}a^v_{i'+1}}{2^n}\right)\left(1-\frac{2\sum_{i'=c+c_6}^{c+c_6+c_7-1}a^y_{i'+1}}{2^n}\right)\geqslant 1-\frac{2\sum_{i'=c}^{c+c_6-1}a^v_{i'+1}+2\sum_{i'=c+c_6}^{c+c_6+c_7-1}a^y_{i'+1}}{2^n}.\end{aligned}$$

于是, 根据 $a^v_{i'+1}+a^y_{i'+1}=a_{i'+1}$, $\sum_{i=1}^{c+c_6+c_7}a_i\leqslant q_a$ 并令 $q'=q_2+\alpha+c_3+q_4+q_5+c_6$ 且 $q''=q_1+\alpha+q_3+c_4+q_5+c_7$, 进一步计算可得图 G 所有可能的解数 $h(G)$ 的下界:

$$\begin{aligned}&h(G)\frac{\prod_{i=1}^{c+c_6+c_7}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}\\&\geqslant\frac{h(c_1+c_2)\prod_{i=1}^{c_1+c_2}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}{(2^n-p_1)_{q_2}(2^n-p_2)_{q_1}}\cdot\sum_{\alpha=1}^{M}\frac{N_S(\alpha)\prod_{i=1}^{\alpha}(2^n-\delta_i)}{(2^n-p_1-q_2)_\alpha(2^n-p_2-q_1)_\alpha}\\&\quad\cdot\frac{h_C(c_3+c_4)\prod_{i=c_1+c_2+\alpha+1}^{c_1+c_2+\alpha+c_3+c_4}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}{(2^n-p_1-q_2-\alpha)_{c_3+q_4}(2^n-p_2-q_1-\alpha)_{q_3+c_4}}\\&\quad\cdot\frac{h_D(c_5)\prod_{i''=c'+1}^{c'+c_5}(2^n-\delta_i)}{(2^n-p_1-q_2-\alpha-c_3-q_4)_{q_5}(2^n-p_2-q_1-\alpha-q_3-c_4)_{q_5}}\\&\quad\cdot\frac{h_E(c_6+c_7)}{(2^n-p_1-q_2-\alpha-c_3-q_4-q_5)_{c_6}(2^n-p_2-q_1-\alpha-q_3-c_4-q_5)_{c_7}}\\&\geqslant 1-\frac{\sum_{i=1}^{c_1+c_2}\delta}{2^n}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+q_2+p_2+q_1)}{q_m2^{2n/3}}-\frac{2\delta}{2^n}\\&\quad-\frac{\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}2\eta_{i+1}^2(p_1+q_m)^2+\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}2\eta_{i+1}(p_1+q_m)(p_2+q_m)+2(c_3+c_4)\delta^2}{2^{2n}}\\&\quad-\frac{\sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}2\eta_{i+1}^2(p_2+q_m)^2}{2^{2n}}-\frac{2\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}a_{i+1}}{2^n}\end{aligned}$$

$$
\begin{aligned}
&-\frac{2c_5(p_1+q_m)(p_2+q_m)+2c_5\delta^2}{2^{2n}}-\frac{2\sum_{i''=c'+1}^{c'+c_5}a_{i''+1}}{2^n}-\frac{2\sum_{i'=c}^{c+c_6-1}a^v_{i'+1}+2\sum_{i'=c+c_6}^{c+c_6+c_7-1}a^y_{i'+1}}{2^n}\\
\geqslant&1-\frac{2(p_1+q_m)^2\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}\eta_{i+1}^2+2(p_2+q_m)^2\sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}^2}{2^{2n}}\\
&-\frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}+c_5)}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\\
&-\frac{2(c_3+c_4+c_5)\delta^2}{2^{2n}}-\frac{\sum_{i=1}^{c_1+c_2}\delta}{2^n}-\frac{2\delta}{2^n}-\frac{2q_a}{2^n}.
\end{aligned}
$$

于是, 对于带有不等式约束的强 (可调) 伪随机置换假设下镜像系统 $G(\mathcal{E}^{p_1,p_2})$ 的所有可能解的个数至少为

$$
\begin{aligned}
h(G)\geqslant&\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{\prod_{i=1}^{c+c_6+c_7}\prod_{j=1}^{\eta_i}(2^n-\delta_i^j)}\left(1-\frac{2(p_1+q_m)^2\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}\eta_{i+1}^2+2(p_2+q_m)^2\sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}^2}{2^{2n}}\right.\\
&-\frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}+c_5)}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\\
&\left.-\frac{2(c_3+c_4+c_5)\delta^2}{2^{2n}}-\frac{\sum_{i=1}^{c_1+c_2}\delta}{2^n}-\frac{2\delta}{2^n}-\frac{2q_a}{2^n}\right).
\end{aligned}
$$

对于带有不等式约束的 (可调) 伪随机函数或消息认证码假设下镜像系统 $G(\mathcal{E}^{p_1,p_2})$ 的所有可能解的个数至少为

$$
\begin{aligned}
h(G)\geqslant&\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{2^{nq_m}}\left(1-\frac{2(p_1+q_m)^2\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3-1}\eta_{i+1}^2+2(p_2+q_m)^2\sum_{i=c_1+c_2+\alpha+c_3}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}^2}{2^{2n}}\right.\\
&\left.-\frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2+\alpha}^{c_1+c_2+\alpha+c_3+c_4-1}\eta_{i+1}+c_5)}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}-\frac{2q_a}{2^n}\right).
\end{aligned}
$$

与陈玉龙 [19] 给出的结果相比较, 本文改进的结果更细粒度地刻画了基于随机置换模型下的拓展镜像理论系统的解个数的下界, 不但囊括了不同随机置换的差异性 (即下界表达式中含有 p_1 和 p_2 的参数项), 而且允许随机置换构成的顶点集存在交集 (即下界表达式中含有 α 且 $\alpha\geqslant 0$), 这在实际案例中具有更广泛的应用空间.

4　基于可调 Even-Mansour 密码实例构造超生日界安全的可调密码方案

超生日界安全的可调密码方案通常可以使用以下两种方法构造, 一是基于伪随机置换或公开置换的异或和 (并联模式) 构造, 二是基于伪随机置换或公开置换的级联接 (串联模式) 构造. 当然, 除了这两种通用的设计方法之外, 也还有其他的设计思路, 如截取的设计以及其他设计. 这里我们基于可调 Even-Mansour 密码实例的并联和串联模式分别构造超生日界安全的可调密码本原.

4.1　基于可调 Even-Mansour 密码实例的并联模式构造的超生日界安全的可调伪随机函数

令 P_1 和 P_2 是两个独立的 n 比特公共置换, K_1 和 K_2 是两个独立的密钥, t 是调柄, h 是 ϵ_1-近乎均匀且 ϵ_2-AXU 泛哈希函数, 则对于输入 t, x 和输出 y, 基于两个可调 Even-Mansour 密码实例的异或和构造的可调伪随机函数 SoTEM 被定义为

$$
y=\mathrm{SoTEM}_{K_1,K_2}^{P_1,P_2,h}(t,x)=P_1(x\oplus h_{K_1}(t))\oplus P_2(x\oplus h_{K_2}(t))\oplus h_{K_1}(t)\oplus h_{K_2}(t).
$$

SoTEM 的并联结构如图 2 所示.

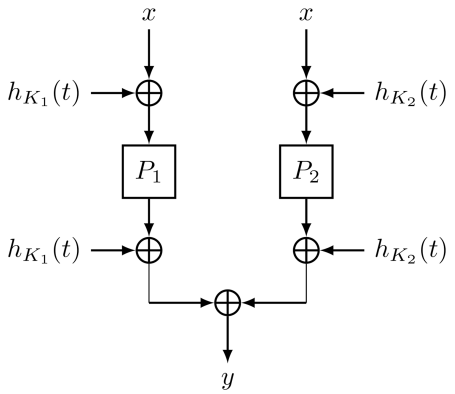

图 2　SoTEM: 基于可调 Even-Mansour 密码实例的异或和构造的超生日界安全的可调伪随机函数.

Figure 2　SoTEM: beyond-birthday-bound (BBB) secure tweakable pseudorandom function constructed by the summation of tweakable Even-Mansour cipher instances.

定理2　如果敌手 $\mathcal{A}$ 做 q_m 次构造查询, p_1 次公共置换 P_1 查询和 p_2 次公共置换 P_2 查询, 则 SoTEM 的可调伪随机函数优势为

$$\begin{aligned}\mathrm{Adv}^{\mathrm{tprf}}_{\mathrm{SoTEM}}(\mathcal{A}) \leqslant & \frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m 2^{n/3}}\\ & +3q_m p_1 p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.\end{aligned}$$

证明　令 P_1, P_2 是从 n 比特置换簇 $\mathrm{Perm}(n)$ 中随机选取的, 令 $\widetilde{F}$ 是一个从 n 比特可调函数族 $\widetilde{\mathrm{Func}}(\Gamma,n)$ 中随机选取的, 其中 Γ 是调柄空间. 假设 $\mathcal{A}$ 是一个确定性对手, 它能查询真实构造方案 SoTEM 或理想方案 $\widetilde{F}$, 也能查询公共置换 P_1 和公共置换 P_2, 并将交互过程记作 $\mathcal{A}^{\mathrm{SoTEM};P_1^{\pm},P_2^{\pm}}$ 或者 $\mathcal{A}^{\widetilde{F};P_1^{\pm},P_2^{\pm}}$, 其中 $P_1^{\pm},P_2^{\pm}$ 表示敌手 $\mathcal{A}$ 可以对公共置换 P_1 和 P_2 做双向查询. 假设敌手 $\mathcal{A}$ 做 q_m 次构造查询, 并将与真实构造方案 SoTEM 或理想方案 $\widetilde{F}$ 交互查询应答对记作脚本 $\tau_{q_m}=\{(t_1,x_1,y_1),\ldots,(t_{q_m},x_{q_m},y_{q_m})\}$; 做 p_1 次公共置换 P_1 查询, 并将交互查询应答对记作脚本 $\tau_{p_1}=\{(u_{1,1},v_{1,1}),\ldots,(u_{1,p_1},v_{1,p_1})\}$; 做 p_2 次公共置换 P_2 查询, 并将交互查询应答对记作脚本 $\tau_{p_2}=\{(u_{2,1},v_{2,1}),\ldots,(u_{2,p_2},v_{2,p_2})\}$. 为了不失一般性, 我们假设敌手每次查询的输入值都不同, 即对于 $1\leqslant i\neq j\leqslant q_m$ 都有 $(t_i,x_i)\neq(t_j,x_j)$; 对于 $1\leqslant i\neq j\leqslant p_1$ 都有 $u_{1,i}\neq u_{1,j}$ 和 $v_{1,i}\neq v_{1,j}$; 对于 $1\leqslant i\neq j\leqslant p_2$ 都有 $u_{2,i}\neq u_{2,j}$ 和 $v_{2,i}\neq v_{2,j}$. 我们将总的脚本记录记为 $\tau=(\tau_{q_m},\tau_{p_1},\tau_{p_2})$.

令 $X_i=x_i\oplus h_{K_1}(t_i)$, $Y_i=x_i\oplus h_{K_2}(t_i)$, 以及 $Z_i=y_i\oplus h_{K_1}(t_i)\oplus h_{K_2}(t_i)$, 则脚本 τ_{q_m}, τ_{p_1} 和 τ_{p_2} 分别定义了如下 $q_m+p_1+p_2$ 个等式方程组:

$$\mathcal{E}_m:\begin{cases}P_1(X_1)\oplus P_2(Y_1)=Z_1,\\ P_1(X_2)\oplus P_2(Y_2)=Z_2,\\ \quad\vdots\\ P_1(X_{q_m})\oplus P_2(Y_{q_m})=Z_{q_m},\end{cases}\quad \mathcal{E}_{p_1}:\begin{cases}P_1(u_{1,1})=v_{1,1},\\ P_1(u_{1,2})=v_{1,2},\\ \quad\vdots\\ P_1(u_{1,p_1})=v_{1,p_1},\end{cases}\quad \mathcal{E}_{p_2}:\begin{cases}P_2(u_{2,1})=v_{2,1},\\ P_2(u_{2,2})=v_{2,2},\\ \quad\vdots\\ P_2(u_{2,p_2})=v_{2,p_2}.\end{cases}$$

由于 P_1 和 P_2 是随机选取的, 因此对于任意 $1\leqslant i,\ j\leqslant q_m$, 都有 $P_1(X_i)\neq P_2(Y_j)$, 即 $\{P_1(X_i)\}_{i=1}^{q_m}\cap\{P_2(Y_j)\}_{j=1}^{q_m}=\emptyset$. 对于 $1\leqslant i,j\leqslant q_m$, 可能存在 $X_i=X_j$, $Y_i=Y_j$; 对于 $1\leqslant i\leqslant q_m$, $1\leqslant j\leqslant q_1$, 可能存在 $X_i=u_{1,j}$, $Y_i=u_{2,j}$. 因此, 需要从总的查询数中去掉这些碰撞查询. 令 $U_1=\{u_{1,i}:(u_{1,i},v_{1,i})\in\tau_{p_1}\}$, $V_1=\{v_{1,i}:(u_{1,i},v_{1,i})\in\tau_{p_1}\}$, $U_2=\{u_{2,i}:(u_{2,i},v_{2,i})\in\tau_{p_2}\}$, $V_2=\{v_{2,i}:(u_{2,i},v_{2,i})\in\tau_{p_2}\}$. 令 $\alpha_1=|\{(t,x,y)\in\tau_{q_m}:X=x\oplus h_{K_1}(t)\in U_1\}|$, $\alpha_2=|\{(t,x,y)\in\tau_{q_m}:Y=x\oplus h_{K_2}(t)\in U_2\}|$, $\beta_1=|\{X=x\oplus h_{K_1}(t):(t,x,y)\in\tau_{q_m}\}|$, $\beta_2=|\{Y=x\oplus h_{K_2}(t):(t,x,y)\in\tau_{q_m}\}|$, 并且有界. 因此, 需要定义一个 "坏" 的脚本记录.

定义3 ("坏" 的脚本记录)　对于一个脚本记录 τ, 如果下列任一条件成立时, 那么我们称 τ 是 "坏" 的.

(1) 一个构造查询与两个置换查询碰撞.

• Bad1. 存在 $(t_i, x_i, y_i) \in \tau_{q_m}$ 以及 $(u_{1,j}, v_{1,j}) \in \tau_{p_1}$ 和 $(u_{2,k}, v_{2,k}) \in \tau_{p_2}$ 使得 $X_i = u_{1,j}$, $Y_i = u_{2,k}$.

• Bad2. 存在 $(t_i, x_i, y_i) \in \tau_{q_m}$ 以及 $(u_{1,j}, v_{1,j}) \in \tau_{p_1}$ 和 $(u_{2,k}, v_{2,k}) \in \tau_{p_2}$ 使得 $X_i = u_{1,j}$, $v_{1,j} \oplus Z_i = v_{2,k}$.

• Bad3. 存在 $(t_i, x_i, y_i) \in \tau_{q_m}$ 以及 $(u_{1,j}, v_{1,j}) \in \tau_{p_1}$ 和 $(u_{2,k}, v_{2,k}) \in \tau_{p_2}$ 使得 $Y_i = u_{2,k}$, $v_{2,k} \oplus Z_i = v_{1,j}$.

(2) 两个构造查询之间碰撞.

• Bad4. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 使得 $X_i = X_j$, $Z_i = Z_j$.

• Bad5. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 使得 $Y_i = Y_j$, $Z_i = Z_j$.

(3) 两个构造查询和一个置换查询碰撞.

• Bad6. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 以及 $(u_{1,k}, v_{1,k}) \in \tau_{p_1}$ 使得 $X_i = u_{1,k}$, $Y_i = Y_j$.

• Bad7. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 以及 $(u_{2,k}, v_{2,k}) \in \tau_{p_2}$ 使得 $Y_i = u_{2,k}$, $X_i = X_j$.

(4) 两个构造查询和两个置换查询碰撞.

• Bad8. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 以及 $(u_{1,k}, v_{1,k}) \neq (u_{1,l}, v_{1,l}) \in \tau_{p_1}$ 使得 $X_i = u_{1,k}, X_j = u_{1,l}$, $v_{1,k} \oplus Z_i = v_{1,l} \oplus Z_j$.

• Bad9. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \in \tau_{q_m}$ 以及 $(u_{2,k}, v_{2,k}) \neq (u_{2,l}, v_{2,l}) \in \tau_{p_2}$ 使得 $Y_i = u_{2,k}, Y_j = u_{2,l}$, $v_{2,k} \oplus Z_i = v_{2,l} \oplus Z_j$.

(5) 3 个构造查询之间碰撞.

• Bad10. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \neq (t_k, x_k, y_k) \in \tau_{q_m}$ 使得 $X_i = X_j$, $Y_i = Y_k$.

• Bad11. 存在 $(t_i, x_i, y_i) \neq (t_j, x_j, y_j) \neq (t_k, x_k, y_k) \in \tau_{q_m}$ 使得 $Z_i = Z_j$, $Z_i = Z_k$.

(6) 其他坏的条件.

• Bad12. $\alpha_1 \geqslant \sqrt{q_m}$.

• Bad13. $\alpha_2 \geqslant \sqrt{q_m}$.

• Bad14. $\beta_1 \geqslant \sqrt{q_m}$.

• Bad15. $\beta_2 \geqslant \sqrt{q_m}$.

令 Ω 表示所有可获得的脚本记录集合, Ω_{bad} 表示所有 "坏" 的脚本记录集合, $\Omega_{\text{good}} = \Omega \setminus \Omega_{\text{bad}}$.

下面, 我们根据 H 系数技术 (引理 1), 先给出理想方案中 "坏" 的脚本记录发生的概率. 在理想方案中, K_1 和 K_2 是从密钥空间随机选择的虚拟密钥. 于是, 各个 "坏" 的脚本记录发生的概率计算如下.

首先, 对于 Bad1, 根据哈希函数的性质 (ϵ_1-AU 且 ϵ_2-AXU 泛哈希), 有

$$\begin{aligned}\Pr[\text{Bad1}] =& \sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[X_i = u_{1,j}, Y_i = u_{2,k}] = \sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[x_i \oplus h_{K_1}(t_i) = u_{1,j}, x_i \oplus h_{K_2}(t_i) = u_{2,k}]\\ \leqslant& q_m p_1 p_2 \epsilon_1^2.\end{aligned}$$

对于 Bad2 和 Bad3, 根据哈希函数的性质 (ϵ_1-AU 且 ϵ_2-AXU 泛哈希) 和条件概率公式, 可以得到

$$\begin{aligned}\Pr[\text{Bad2}] =& \sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[X_i = u_{1,j}, v_{1,j} \oplus Z_i = v_{2,k}]\\ =& \sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[x_i \oplus h_{K_1}(t_i) = u_{1,j}, v_{1,j} \oplus y_i \oplus h_{K_1}(t_i) \oplus h_{K_2}(t_i) = v_{2,k}] \leqslant q_m p_1 p_2 \epsilon_1^2,\end{aligned}$$

$$\begin{aligned}\Pr[\text{Bad3}] =&\sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[Y_i = u_{2,j}, v_{1,j}\oplus Z_i = v_{2,k}]\\ =&\sum_{i=1}^{q_m}\sum_{j=1}^{p_1}\sum_{k=1}^{p_2}\Pr[x_i\oplus h_{K_2}(t_i) = u_{2,j}, v_{1,j}\oplus y_i\oplus h_{K_1}(t_i)\oplus h_{K_2}(t_i) = v_{2,k}]\leqslant q_m p_1 p_2\epsilon_1^2.\end{aligned}$$

类似地, 对于 Bad4∼Bad11, 根据哈希函数的性质 (ϵ_1-AU 且 ϵ_2-AXU 泛哈希), 有

$$\begin{aligned}&\Pr[\text{Bad4}]\leqslant q_m^2\epsilon_2^2,\ \Pr[\text{Bad5}]\leqslant q_m^2\epsilon_2^2,\ \Pr[\text{Bad6}]\leqslant q_m^2 p_1\epsilon_1\epsilon_2,\ \Pr[\text{Bad7}]\leqslant q_m^2 p_2\epsilon_1\epsilon_2,\\ &\Pr[\text{Bad8}]\leqslant q_m^2 p_1^2\epsilon_1^2\epsilon_2,\ \Pr[\text{Bad9}]\leqslant q_m^2 p_2^2\epsilon_1^2\epsilon_2,\ \Pr[\text{Bad10}]\leqslant q_m^3\epsilon_2^2,\ \Pr[\text{Bad11}]\leqslant q_m^3\epsilon_2^2.\end{aligned}$$

对于 Bad12∼Bad15, 根据马尔可夫 (Markov) 不等式 $\Pr[X\geqslant a]\leqslant\frac{E[X]}{a}$, 有

$$\begin{aligned}\Pr[\text{Bad12}] =&\Pr[\alpha_1\geqslant\sqrt{q_m}]\leqslant\frac{E[\alpha_1]}{\sqrt{q_m}}\leqslant\frac{q_m p_1/2^n}{\sqrt{q_m}}\leqslant\frac{p_1\sqrt{q_m}}{2^n},\\ \Pr[\text{Bad13}] =&\Pr[\alpha_2\geqslant\sqrt{q_m}]\leqslant\frac{E[\alpha_2]}{\sqrt{q_m}}\leqslant\frac{p_2\sqrt{q_m}}{2^n},\\ \Pr[\text{Bad14}] =&\Pr[\beta_1\geqslant\sqrt{q_m}]\leqslant\frac{E[\beta_1]}{\sqrt{q_m}}\leqslant\frac{q_m^2/2^{n+1}}{\sqrt{q_m}}\leqslant\frac{q_m\sqrt{q_m}}{2^{n+1}},\\ \Pr[\text{Bad15}] =&\Pr[\beta_2\geqslant\sqrt{q_m}]\leqslant\frac{E[\beta_2]}{\sqrt{q_m}}\leqslant\frac{q_m\sqrt{q_m}}{2^{n+1}}.\end{aligned}$$

综上所述, 在理想系统中, "坏" 的脚本记录的概率为

$$\begin{aligned}\Pr[X_{\text{id}}\in\Omega_{\text{bad}}] =&\Pr\left[\bigcup_{i=1}^{15}\text{Bad}i\right]\leqslant\sum_{i=1}^{15}\Pr[\text{Bad}i]\\ \leqslant&\frac{(p_1+p_2+q_m)\sqrt{q_m}}{2^n}+3q_m p_1 p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.\end{aligned}$$

在 "好" 的脚本记录下, 上面描述的等式方程组系统对应改进的随机置换模型下的拓展镜像系统 $G(\mathcal{E}_m^{p_1,p_2})$, 并具有如下性质.

• 无圈性. 图 $G(\mathcal{E}_m^{p_1,p_2})$ 中任意一个连通分支上的任两个顶点 $a,b\in V^{p_1}\cup Y^{p_2}$ 之间只存在一条唯一的路径, 否则满足 Bad10 和 Bad11.

• 连通分支顶点数 $\xi_{\max}$ 有界并且 $\xi_{\max}=\beta_1+\beta_2\leqslant 2\sqrt{q_m}$, 否则满足 Bad14 和 Bad15.

• 不可退化 (非零路径标签). 图 $G(\mathcal{E}_m^{p_1,p_2})$ 中不存在任何一条偶数长路径 $\mathcal{P}$ 使得 $L(\mathcal{P})=0$, 否则满足 Bad4, Bad5, Bad10 和 Bad11.

• 单碰撞顶点. 在 $G(\mathcal{E}_m^{p_1,p_2})$ 每个连通分支中最多包含一个碰撞独立顶点, 否则满足 Bad1∼Bad3, Bad6∼Bad9, Bad12 和 Bad13.

根据改进的随机置换模型下的拓展镜像理论, 图 $G(\mathcal{E}_m^{p_1,p_2})$ 可以划分为 P_1 和 P_2 生成的独立顶点集 I、c_1 个与 P_1 生成的独立顶点集碰撞的连通分支 $A_1,\ldots,A_{c_1}$、c_2 个与 P_2 生成的独立顶点集碰撞的连通分支 $A_{c_1+1},\ldots,A_{c_1+c_2}$、$c_3$ 个与 P_1 生成的独立顶点集不碰撞的星型连通分支 $B_1,\ldots,B_{c_3}$、c_4 个与 P_1 生成的独立顶点集不碰撞的星型连通分支 $B_{c_3+1},\ldots,B_{c_3+c_4}$ 以及 c_5 个不碰撞的单边连通分支 $C_1,\ldots,C_{c_5}$. 令 q_1, q_2, q_3, q_4, q_5 分别表示 $A_1\cup\cdots\cup A_{c_1}$, $A_{c_1+1}\cup\cdots\cup A_{c_1+c_2}$, $B_1\cup\cdots\cup B_{c_3}$, $B_{c_3+1}\cup\cdots\cup B_{c_3+c_4}$ 以及 C 的等边数 (等式的数量). 于是有 $c_1=\alpha_1\leqslant\sqrt{q_m}$, $q_1=\sum_{i=1}^{c_1}\eta_i=\alpha_2\leqslant\sqrt{q_m}$, $c_2=\alpha_2\leqslant\sqrt{q_m}$, $q_2=\sum_{i=c_1+1}^{c_1+c_2}\eta_i=\alpha_1\leqslant\sqrt{q_m}$, $c_3\leqslant\beta_1\leqslant\sqrt{q_m}$, $q_3=\sum_{i=c_1+c_2+1}^{c_1+c_2+c_3}\eta_i\leqslant\beta_1\leqslant\sqrt{q_m}$, $c_4\leqslant\beta_2\leqslant\sqrt{q_m}$, $q_4=\sum_{i=c_1+c_2+c_3+1}^{c_1+c_2+c_3+c_4}\eta_i\leqslant\beta_2\leqslant\sqrt{q_m}$, $q_5=c_5$ 并且 $\sum_{i=1}^{c_1+c_2+c_3+c_4+c_5}\eta_i=q_1+q_2+q_3+q_4+q_5=q_m$.

令 $q'=q_2+c_3+q_4+q_5$ 和 $q''=q_1+q_3+c_4+q_5$, 根据定理 1, 真实方案 SoTEM 导出的改进的拓展镜像系统解的个数至少是

$$\begin{aligned}
&\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{2^{nq_m}}\left(1-\frac{2(p_1+q_m)^2\sum_{i=c_1+c_2}^{c_1+c_2+c_3-1}\eta_{i+1}^2+2(p_2+q_m)^2\sum_{i=c_1+c_2+c_3}^{c_1+c_2+c_3+c_4-1}\eta_{i+1}^2}{2^{2n}}\right.\\
&\quad\left.-\frac{2(p_1+q_m)(p_2+q_m)(\sum_{i=c_1+c_2}^{c_1+c_2+c_3+c_4-1}\eta_{i+1}+c_5)}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\right)\\
\geqslant&\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{2^{nq_m}}\left(1-\frac{2(p_1+q_m)^2q_m+2(p_2+q_m)^2q_m}{2^{2n}}-\frac{4q_m(p_1+q_m)(p_2+q_m)}{2^{2n}}\right.\\
&\quad\left.-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\right)\\
=&\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{2^{nq_m}}\left(1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\right).
\end{aligned}$$

因此, 真实方案 SoTEM 在好的脚本 τ 下, 有

$$\begin{aligned}
\Pr[X_{\rm re}=\tau]&=\Pr[K_1,K_2\xleftarrow{\$}\mathcal{K}]\cdot\Pr[P_1,P_2\xleftarrow{\$}\mathrm{Perm}(n):P_1\vdash\tau_{p_1},P_2\vdash\tau_{p_2}]\cdot\Pr[\mathrm{SoTEM}\vdash\tau_{q_m}]\\
&\geqslant\frac{1}{|\mathcal{K}|^2}\cdot\frac{1}{(2^n)_{p_1}}\cdot\frac{1}{(2^n)_{p_2}}\cdot\frac{1}{2^{nq_m}}\left(1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\right).
\end{aligned}$$

对于理想方案 $\widetilde{F}$ 在好的脚本 τ 下, 根据 $\sum_{t\in\Gamma}q_t=q_m$ (这里 q_t 表示调柄 t 被使用的次数), 有

$$\begin{aligned}
\Pr[X_{\rm id}=\tau]&=\Pr[K_1,K_2\xleftarrow{\$}\mathcal{K}]\cdot\Pr[P_1,P_2\xleftarrow{\$}\mathrm{Perm}(n):P_1\vdash\tau_{p_1},P_2\vdash\tau_{p_2}]\cdot\Pr[\widetilde{F}\xleftarrow{\$}\widetilde{\mathrm{Func}}(\Gamma,n):\widetilde{F}\vdash\tau_{q_m}]\\
&=\frac{1}{|\mathcal{K}|^2}\cdot\frac{1}{(2^n)_{p_1}}\cdot\frac{1}{(2^n)_{p_2}}\cdot\frac{1}{\prod_{t\in\Gamma}(2^n)^{q_t}}=\frac{1}{|\mathcal{K}|^2}\cdot\frac{1}{(2^n)_{p_1}}\cdot\frac{1}{(2^n)_{p_2}}\cdot\frac{1}{2^{nq_m}}.
\end{aligned}$$

于是, 在好的脚本 τ 下, 有

$$\frac{\Pr[X_{\rm re}=\tau]}{\Pr[X_{\rm id}=\tau]}\geqslant1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}.$$

根据 H 系数技术引理 (引理 1), 有

$$\begin{aligned}
\mathrm{Adv}^{\rm tprf}_{\rm SoTEM}(\mathcal{A})\leqslant&\frac{(p_1+p_2+q_m)\sqrt{q_m}}{2^n}+3q_mp_1p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2\\
&+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2+\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\\
\leqslant&\frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}\\
&+3q_mp_1p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.
\end{aligned}$$

定理 2 的结论得证.

定理 2 的结果表明, SoTEM 是可证明超生日界安全的可调伪随机函数, 在 $\epsilon_1=\epsilon_2=2^{-n}$ 情况下, 它能够抵抗 $O(2^{2n/3})$ 敌手构造查询和底层置换本原查询, 即确保了 $2n/3$ 比特的安全性.

特别地, 如果 $h_{K_1}(t)=K_1,\ h_{K_2}(t)=K_2$, 此时 $\epsilon_1=\epsilon_2=2^{-n}$, SoTEM 将退化为 SoEM22 [9], 即

$$y=\mathrm{SoEM22}^{P_1,P_2}_{K_1,K_2}(x)=P_1(x\oplus K_1)\oplus P_2(x\oplus K_2)\oplus K_1\oplus K_2.$$

推论1　如果敌手 $\mathcal{A}$ 做 q_m 次 SoEM22 构造查询, p_1 次公共置换 P_1 查询和 p_2 次公共置换 P_2 查询, 则 SoEM22 的伪随机函数优势为

$$\mathrm{Adv}^{\rm prf}_{\rm SoEM22}(\mathcal{A})\leqslant\frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}$$

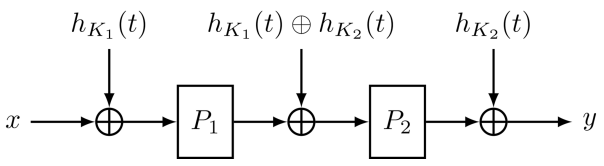

图 3　CoTEM: 基于可调 Even-Mansour 密码实例的级联接构造的超生日界安全的强可调伪随机置换.

Figure 3　CoTEM: BBB secure strong tweakable pseudorandom permutation constructed by the cascade of tweakable Even-Mansour cipher instances.

$$+\frac{3q_mp_1p_2+2q_m^2+q_m^2(p_1+p_2)+2q_m^3}{2^{2n}}+\frac{q_m^2(p_1^2+p_2^2)}{2^{3n}}.$$

推论 1 的结果验证了 SoEM22 是可证明超生日界安全的伪随机函数, 它能够抵抗 $O(2^{2n/3})$ 敌手构造查询和底层置换查询, 即确保了 $2n/3$ 比特的安全性. 与以前的结果相比较 [9], 我们的结果更加精细和准确地展现了伪随机函数安全性.

4.2　基于可调 Even-Mansour 密码实例的级联模式构造的超生日界安全的强可调伪随机置换

令 P_1 和 P_2 是两个独立的 n 比特公共置换, K_1 和 K_2 是两个独立的密钥, t 是调柄, h 是 ϵ_1-近乎均匀且 ϵ_2-AXU 泛哈希函数, 则对于输入 t,x 和输出 y, 基于两个可调 Even-Mansour 密码实例的级联接构造的强可调伪随机置换 CoTEM 被定义为

$$y=\mathrm{CoTEM}_{K_1,K_2}^{P_1,P_2,h}(t,x)=P_2(P_1(x\oplus h_{K_1}(t))\oplus h_{K_1}(t)\oplus h_{K_2}(t))\oplus h_{K_2}(t).$$

CoTEM 的级联结构如图 3 所示.

定理3　如果敌手 $\mathcal{A}$ 做 q_m 次构造查询, p_1 次公共置换 P_1 查询和 p_2 次公共置换 P_2 查询, 则 CoTEM 的强可调伪随机置换优势为

$$\begin{aligned}\mathrm{Adv}_{\mathrm{CoTEM}}^{\mathrm{stprp}}(\mathcal{A})\leqslant&\frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}+\frac{2q_m}{2^n}\\&+3q_mp_1p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.\end{aligned}$$

证明　定理 3 的证明与陈玉龙 [19] 论文证明基本一致, 除了考虑两个随机置换查询的差异性. 令 P_1,P_2 是从 n 比特置换簇 $\mathrm{Perm}(n)$ 中随机选取的, 令 $\widetilde{P}$ 是一个从 n 比特可调置换族 $\widetilde{\mathrm{Perm}}(\Gamma,n)$ 中随机选取的, 其中 Γ 是调柄空间. 假设 $\mathcal{A}$ 是一个确定性对手, 它能查询真实构造方案 CoTEM 或理想方案 $\widetilde{P}$, 也能查询公共置换 P_1 和公共置换 P_2, 并将交互过程记作 $\mathcal{A}^{\mathrm{CoTEM}^{\pm};P_1^{\pm},P_2^{\pm}}$ 或者 $\mathcal{A}^{\widetilde{P}^{\pm};P_1^{\pm},P_2^{\pm}}$, 其中 $\pm$ 表示敌手 $\mathcal{A}$ 可以对置换做双向查询. 假设敌手 $\mathcal{A}$ 做 q_m 次构造查询, 并将与真实构造方案 CoTEM 或理想方案 $\widetilde{P}$ 交互查询应答对记作脚本 $\tau_{q_m}=\{(t_1,x_1,y_1),\ldots,(t_{q_m},x_{q_m},y_{q_m})\}$; 做 p_1 次公共置换 P_1 查询, 并将交互查询应答对记作脚本 $\tau_{p_1}=\{(u_{1,1},v_{1,1}),\ldots,(u_{1,p_1},v_{1,p_1})\}$; 做 p_2 次公共置换 P_2 查询, 并将交互查询应答对记作脚本 $\tau_{p_2}=\{(u_{2,1},v_{2,1}),\ldots,(u_{2,p_2},v_{2,p_2})\}$. 为了不失一般性, 我们假设敌手每次查询的输入值都不同, 即对于 $1\leqslant i\neq j\leqslant q_m$ 都有 $(t_i,x_i)\neq(t_j,x_j)$ 和 $(t_i,y_i)\neq(t_j,y_j)$; 对于 $1\leqslant i\neq j\leqslant p_1$ 都有 $u_{1,i}\neq u_{1,j}$ 和 $v_{1,i}\neq v_{1,j}$; 对于 $1\leqslant i\neq j\leqslant p_2$ 都有 $u_{2,i}\neq u_{2,j}$ 和 $v_{2,i}\neq v_{2,j}$. 我们将总的脚本记录记为 $\tau=(\tau_{q_m},\tau_{p_1},\tau_{p_2})$.

令 $X_i=x_i\oplus h_{K_1}(t_i)$, $Y_i=y_i\oplus h_{K_2}(t_i)$, 以及 $Z_i=h_{K_1}(t_i)\oplus h_{K_2}(t_i)$, 则脚本 τ_{q_m}, τ_{p_1} 和 τ_{p_2} 分别

定义了如下 $q_m+p_1+p_2$ 个等式方程组:

$$\mathcal{E}_m:\begin{cases}P_1(X_1)\oplus P_2^{-1}(Y_1)=Z_1,\\ P_1(X_2)\oplus P_2^{-1}(Y_2)=Z_2,\\ \quad\vdots\\ P_1(X_{q_m})\oplus P_2^{-1}(Y_{q_m})=Z_{q_m},\end{cases}\quad \mathcal{E}_{p_1}:\begin{cases}P_1(u_{1,1})=v_{1,1},\\ P_1(u_{1,2})=v_{1,2},\\ \quad\vdots\\ P_1(u_{1,p_1})=v_{1,p_1},\end{cases}\quad \mathcal{E}_{p_2}:\begin{cases}P_2(u_{2,1})=v_{2,1},\\ P_2(u_{2,2})=v_{2,2},\\ \quad\vdots\\ P_2(u_{2,p_2})=v_{2,p_2}.\end{cases}$$

由于 P_1 和 P_2 是随机选取的, 因此对于任意 $1\leqslant i,j\leqslant q_m$, 都有 $P_1(X_i)\neq P_2^{-1}(Y_j)$, 即 $\{P_1(X_i)\}_{i=1}^{q_m}\cap\{P_2^{-1}(Y_j)\}_{j=1}^{q_m}=\emptyset$. 对于 $1\leqslant i,j\leqslant q_m$, 可能存在 $X_i=X_j$, $Y_i=Y_j$; 对于 $1\leqslant i\leqslant q_m$, $1\leqslant j\leqslant q_1$, 可能存在 $X_i=u_{1,j}$, $Y_i=v_{2,j}$. 因此, 需要从总的查询数中去掉这些碰撞查询. 令 $U_1=\{u_{1,i}:(u_{1,i},v_{1,i})\in\tau_{p_1}\}$, $V_1=\{v_{1,i}:(u_{1,i},v_{1,i})\in\tau_{p_1}\}$, $U_2=\{u_{2,i}:(u_{2,i},v_{2,i})\in\tau_{p_2}\}$, $V_2=\{v_{2,i}:(u_{2,i},v_{2,i})\in\tau_{p_2}\}$. 令 $\alpha_1=|\{(t,x,y)\in\tau_{q_m}:X=x\oplus h_{K_1}(t)\in U_1\}|$, $\alpha_2=|\{(t,x,y)\in\tau_{q_m}:Y=y\oplus h_{K_2}(t)\in V_2\}|$, $\beta_1=|\{X=x\oplus h_{K_1}(t):(t,x,y)\in\tau_{q_m}\}|$, $\beta_2=|\{Y=y\oplus h_{K_2}(t):(t,x,y)\in\tau_{q_m}\}|$, 并且有界. 因此, 需要定义一个 "坏" 的脚本记录.

定义4 ("坏" 的脚本记录)　对于一个脚本记录 τ, 如果下列任一条件成立时, 那么我们称 τ 是 "坏" 的.

(1) 一个构造查询与两个置换查询碰撞.

• Bad1. 存在 $(t_i,x_i,y_i)\in\tau_{q_m}$ 以及 $(u_{1,j},v_{1,j})\in\tau_{p_1}$ 和 $(u_{2,k},v_{2,k})\in\tau_{p_2}$ 使得 $X_i=u_{1,j}$, $Y_i=v_{2,k}$.

• Bad2. 存在 $(t_i,x_i,y_i)\in\tau_{q_m}$ 以及 $(u_{1,j},v_{1,j})\in\tau_{p_1}$ 和 $(u_{2,k},v_{2,k})\in\tau_{p_2}$ 使得 $X_i=u_{1,j}$, $v_{1,j}\oplus Z_i=v_{2,k}$.

• Bad3. 存在 $(t_i,x_i,y_i)\in\tau_{q_m}$ 以及 $(u_{1,j},v_{1,j})\in\tau_{p_1}$ 和 $(u_{2,k},v_{2,k})\in\tau_{p_2}$ 使得 $Y_i=v_{2,k}$, $u_{2,k}\oplus Z_i=v_{1,j}$.

(2) 两个构造查询之间碰撞.

• Bad4. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 使得 $X_i=X_j$, $Z_i=Z_j$.

• Bad5. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 使得 $Y_i=Y_j$, $Z_i=Z_j$.

(3) 两个构造查询和一个置换查询碰撞.

• Bad6. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 以及 $(u_{1,k},v_{1,k})\in\tau_{p_1}$ 使得 $X_i=u_{1,k}$, $Y_i=Y_j$.

• Bad7. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 以及 $(u_{2,k},v_{2,k})\in\tau_{p_2}$ 使得 $Y_i=v_{2,k}$, $X_i=X_j$.

(4) 两个构造查询和两个置换查询碰撞.

• Bad8. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 以及 $(u_{1,k},v_{1,k})\neq(u_{1,l},v_{1,l})\in\tau_{p_1}$ 使得 $X_i=u_{1,k}$, $X_j=u_{1,l}$, $v_{1,k}\oplus Z_i=v_{1,l}\oplus Z_j$.

• Bad9. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\in\tau_{q_m}$ 以及 $(u_{2,k},v_{2,k})\neq(u_{2,l},v_{2,l})\in\tau_{p_2}$ 使得 $Y_i=v_{2,k}$, $Y_j=v_{2,l}$, $u_{2,k}\oplus Z_i=u_{2,l}\oplus Z_j$.

(5) 3 个构造查询之间碰撞.

• Bad10. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\neq(t_k,x_k,y_k)\in\tau_{q_m}$ 使得 $X_i=X_j$, $Y_i=Y_k$.

• Bad11. 存在 $(t_i,x_i,y_i)\neq(t_j,x_j,y_j)\neq(t_k,x_k,y_k)\in\tau_{q_m}$ 使得 $Z_i=Z_j$, $Z_i=Z_k$.

(6) 其他坏的条件.

• Bad12. $\alpha_1\geqslant\sqrt{q_m}$.

• Bad13. $\alpha_2\geqslant\sqrt{q_m}$.

• Bad14. $\beta_1\geqslant\sqrt{q_m}$.

• Bad15. $\beta_2\geqslant\sqrt{q_m}$.

令 Ω 表示所有可获得的脚本记录集合, $\Omega_{\rm bad}$ 表示所有 "坏" 的脚本记录集合, $\Omega_{\rm good}=\Omega\setminus\Omega_{\rm bad}$.

与定理 2 的证明类似, 在理想系统中, “坏” 的脚本记录的概率为

$$\begin{aligned}\Pr[X_{\mathrm{id}}\in\Omega_{\mathrm{bad}}]=&\Pr\left[\bigcup_{i=1}^{15}\mathrm{Bad}i\right]\leqslant\sum_{i=1}^{15}\Pr[\mathrm{Bad}i]\\ \leqslant&\frac{(p_1+p_2+q_m)\sqrt{q_m}}{2^n}+3q_mp_1p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.\end{aligned}$$

在 “好” 的脚本记录下, 上面描述的等式方程组系统对应改进的随机置换模型下的拓展镜像系统 $G(\mathcal{E}_m^{p_1,p_2})$, 并具有如下性质.

• 无圈性. 图 $G(\mathcal{E}_m^{p_1,p_2})$ 中任意一个连通分支上的任两个顶点 $a,b\in V^{p_1}\cup Y^{p_2}$ 之间只存在一条唯一的路径, 否则满足 Bad10 和 Bad11.

• 连通分支顶点数 $\xi_{\max}$ 有界并且 $\xi_{\max}=\beta_1+\beta_2\leqslant 2\sqrt{q_m}$, 否则满足 Bad14 和 Bad15.

• 不可退化 (非零路径标签). 图 $G(\mathcal{E}_m^{p_1,p_2})$ 中不存在任何一条偶数长路径 $\mathcal{P}$ 使得 $L(\mathcal{P})=0$, 否则满足 Bad4, Bad5, Bad10 和 Bad11.

• 单碰撞顶点. 在 $G(\mathcal{E}_m^{p_1,p_2})$ 每个连通分支中最多包含一个碰撞独立顶点, 否则满足 Bad1∼Bad3, Bad6∼Bad9, Bad12 和 Bad13.

根据改进的随机置换模型下的拓展镜像理论, 图 $G(\mathcal{E}_m^{p_1,p_2})$ 可以划分为 P_1 和 P_2 生成的独立顶点集 I、c_1 个与 P_1 生成的独立顶点集碰撞的连通分支 $A_1,\dots,A_{c_1}$、c_2 个与 P_2 生成的独立顶点集碰撞的连通分支 $A_{c_1+1},\dots,A_{c_1+c_2}$、$c_3$ 个与 P_1 生成的独立顶点集不碰撞的星型连通分支 $B_1,\dots,B_{c_3}$、c_4 个与 P_1 生成的独立顶点集不碰撞的星型连通分支 $B_{c_3+1},\dots,B_{c_3+c_4}$ 以及 c_5 个不碰撞的单边连通分支 $C_1,\dots,C_{c_5}$. 令 q_1, q_2, q_3, q_4, q_5 分别表示 $A_1\cup\cdots\cup A_{c_1}$, $A_{c_1+1}\cup\cdots\cup A_{c_1+c_2}$, $B_1\cup\cdots\cup B_{c_3}$, $B_{c_3+1}\cup\cdots\cup B_{c_3+c_4}$ 以及 C 的等边数 (等式的数量). 于是有 $c_1=\alpha_1\leqslant\sqrt{q_m}$, $q_1=\sum_{i=1}^{c_1}\eta_i=\alpha_2\leqslant\sqrt{q_m}$, $c_2=\alpha_2\leqslant\sqrt{q_m}$, $q_2=\sum_{i=c_1+1}^{c_1+c_2}\eta_i=\alpha_1\leqslant\sqrt{q_m}$, $c_3\leqslant\beta_1\leqslant\sqrt{q_m}$, $q_3=\sum_{i=c_1+c_2+1}^{c_1+c_2+c_3}\eta_i\leqslant\beta_1\leqslant\sqrt{q_m}$, $c_4\leqslant\beta_2\leqslant\sqrt{q_m}$, $q_4=\sum_{i=c_1+c_2+c_3+1}^{c_1+c_2+c_3+c_4}\eta_i\leqslant\beta_2\leqslant\sqrt{q_m}$, $q_5=c_5$ 并且 $\sum_{i=1}^{c_1+c_2+c_3+c_4+c_5}\eta_i=q_1+q_2+q_3+q_4+q_5=q_m$. 令 q_t 表示调柄 t 被容许使用的次数, 则 $\sum_{t\in\Gamma}q_t=q_m$.

令 $q'=q_2+c_3+q_4+q_5$ 和 $q''=q_1+q_3+c_4+q_5$, 根据定理 1, 真实方案 CoTEM 导出的改进的拓展镜像系统解的个数至少是

$$\frac{(2^n-p_1)_{q'}(2^n-p_2)_{q''}}{\prod_{t\in\Gamma}(2^n)_{q_t}}\left(1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}-\frac{2q_m}{2^n}\right).$$

因此, 真实方案 CoTEM 在好的脚本 τ 下, 有

$$\begin{aligned}&\Pr[X_{\mathrm{re}}=\tau]\\ &=\Pr[K_1,K_2\xleftarrow{\$}\mathcal{K}]\cdot\Pr[P_1,P_2\xleftarrow{\$}\mathrm{Perm}(n):P_1\vdash\tau_{p_1},P_2\vdash\tau_{p_2}]\cdot\Pr[\mathrm{CoTEM}\vdash\tau_{q_m}]\\ &\geqslant\frac{1}{|\mathcal{K}|^2}\cdot\frac{1}{(2^n)_{p_1}}\cdot\frac{1}{(2^n)_{p_2}}\cdot\frac{1}{\prod_{t\in\Gamma}(2^n)_{q_t}}\left(1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}-\frac{2q_m}{2^n}\right).\end{aligned}$$

对于理想方案 $\widetilde{P}$ 在好的脚本 τ 下, 有

$$\begin{aligned}\Pr[X_{\mathrm{id}}=\tau]&=\Pr[K_1,K_2\xleftarrow{\$}\mathcal{K}]\cdot\Pr[P_1,P_2\xleftarrow{\$}\mathrm{Perm}(n):P_1\vdash\tau_{p_1},P_2\vdash\tau_{p_2}]\cdot\Pr[\widetilde{P}\xleftarrow{\$}\widetilde{\mathrm{Perm}}(\Gamma,n):\widetilde{P}\vdash\tau_{q_m}]\\ &=\frac{1}{|\mathcal{K}|^2}\cdot\frac{1}{(2^n)_{p_1}}\cdot\frac{1}{(2^n)_{p_2}}\cdot\frac{1}{\prod_{t\in\Gamma}(2^n)_{q_t}}.\end{aligned}$$

于是, 在好的脚本 τ 下, 有

$$\frac{\Pr[X_{\mathrm{re}}=\tau]}{\Pr[X_{\mathrm{id}}=\tau]}\geqslant 1-\frac{2q_m(p_1+2q_m+p_2)^2}{2^{2n}}-\frac{19q_m}{2^{2n/3}}-\frac{16(p_1+p_2+q_m)}{q_m2^{n/3}}-\frac{2q_m}{2^n}.$$

根据 H 系数技术引理 (引理 1), 有

$$\begin{aligned}\mathrm{Adv}^{\mathrm{stprp}}_{\mathrm{CoTEM}}(\mathcal{A}) \leqslant & \frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m 2^{n/3}}+\frac{2q_m}{2^n}\\ & +3q_m p_1 p_2\epsilon_1^2+2q_m^2\epsilon_2^2+q_m^2(p_1+p_2)\epsilon_1\epsilon_2+q_m^2(p_1^2+p_2^2)\epsilon_1^2\epsilon_2+2q_m^3\epsilon_2^2.\end{aligned}$$

定理 3 的结论得证.

定理 3 的结果表明, CoTEM 是可证明超生日界安全的强可调伪随机置换, 在 $\epsilon_1=\epsilon_2=2^{-n}$ 情况下, 它能够抵抗 $O(2^{2n/3})$ 敌手构造查询和底层置换本原查询, 即确保了 $2n/3$ 比特的安全性. 与以前的结果相比较 [19,25], 我们的结果更细粒度展现了强可调伪随机置换安全性.

特别地, 如果 $h_{K_1}(t)=K_1,\ h_{K_2}(t)=K_2$, 此时有 $\epsilon_1=\epsilon_2=2^{-n}$, CoTEM 将退化为两轮迭代的 Even-Mansour 密码 EM2 [26], 即

$$y=\mathrm{EM2}^{P_1,P_2}_{K_1,K_2}(x)=P_2(P_1(x\oplus K_1)\oplus K_1\oplus K_2)\oplus K_2.$$

推论2　如果敌手 $\mathcal{A}$ 做 q_m 次 EM2 构造查询, p_1 次公共置换 P_1 查询和 p_2 次公共置换 P_2 查询, 则 EM2 的强伪随机置换优势为

$$\begin{aligned}\mathrm{Adv}^{\mathrm{sprp}}_{\mathrm{EM2}}(\mathcal{A}) \leqslant & \frac{3(p_1+p_2+2q_m)\sqrt{q_m}}{2^n}+\frac{19q_m}{2^{2n/3}}+\frac{16(p_1+p_2+q_m)}{q_m 2^{n/3}}+\frac{2q_m}{2^n}\\ & +\frac{3q_m p_1 p_2+2q_m^2+q_m^2(p_1+p_2)+2q_m^3}{2^{2n}}+\frac{q_m^2(p_1^2+p_2^2)}{2^{3n}}.\end{aligned}$$

推论 2 的结果验证了 EM2 是可证明超生日界安全的强伪随机置换, 它能够抵抗 $O(2^{2n/3})$ 敌手构造查询和底层置换查询, 即确保了 $2n/3$ 比特的安全性. 与以前的结果相比较 [26], 我们的结果更加精细和准确地展现了强伪随机置换安全性.

5　讨论

第 4 节讨论了基于两个可调 Even-Mansour 密码实例的异或和或者级联接构造的超生日界安全的可调密码本原设计方案及其安全性证明, 实际上超生日界安全的可调密码本原也可以通过多个可调 Even-Mansour 密码实例的异或和或者级联接构造. 具体设计思路描述如下.

假设 $P_1,P_2,\ldots,P_l$ 是 l 个公开随机置换, $K_1,K_2,\ldots,K_l$ 是 l 个 n 比特密钥, t 是可调调柄, h 是 ϵ_1-近乎均匀且 ϵ_2-AXU 泛哈希函数, 则基于 l 个可调 Even-Mansour 密码实例的异或和构造的超生日界安全的可调伪随机函数 GSoTEM 定义为

$$\begin{aligned}y=&\mathrm{GSoTEM}^{P_1,P_2,\ldots,P_l,h}_{K_1,K_2,\ldots,K_l}(t,x)\\ =&P_1(x\oplus h_{K_1}(t))\oplus P_2(x\oplus h_{K_2}(t))\oplus\cdots\oplus P_l(x\oplus h_{K_1}(t))\oplus h_{K_1}(t)\oplus h_{K_2}(t)\oplus\cdots\oplus h_{K_1}(t).\end{aligned}$$

Lucks 给出了基于 l 个伪随机置换的异或和是超生日界安全的伪随机函数并使用 fair 集合技术证明了其拥有 $\frac{l}{l+1}\cdot n$ 比特的安全性 [5]. 因此, 我们猜想 GSoTEM 是超生日界安全的可调伪随机函数并拥有 $\frac{l}{l+1}\cdot n$ 比特的安全性. 第 3 节提出的改进的随机置换模型下的拓展镜像理论仍然考虑的是二变量镜像理论, 应用在 GSoTEM 的安全性证明中, 需要进行转化. 由于每个 l 变量的仿射等式都需要使用 $l-1$ 个二变量的仿射方程组来描述, 且对输出值引入更多的变量进行了截分, 这使得转化后等式方程组系统分析的过程稍微复杂. 因此, 这里我们将基于多变量的拓展镜像系统超图理论以及如何使用改进的拓展镜像理论证明 GSoTEM 方案确保了 $\frac{l}{l+1}\cdot n$ 比特的安全性作为一个开放性问题遗留下来以期进一步讨论与研究.

类似地, 基于 l 个可调 Even-Mansour 密码实例的级联接构造的超生日界安全的强可调伪随机置换 GCoTEM 定义为

$$\begin{aligned} y =& \mathrm{GCoTEM}^{P_1,P_2,\ldots,P_l,h}_{K_1,K_2,\ldots,K_l}(t,x)\\ =& P_l(\cdots(P_2(P_1(x\oplus h_{K_1}(t))\oplus h_{K_1}(t)\oplus h_{K_2}(t))\oplus h_{K_2}(t))\oplus\cdots\oplus h_{K_l}(t))\oplus h_{K_l}(t). \end{aligned}$$

Cogliati 等 [28] 使用耦合技术和统计距离方法证明了 GCoTEM (即 l 轮的可调 Even-Mansour 密码 TEM-l) 是超生日界安全的, 并给出了 $\frac{l}{l+1}\cdot n$ 比特的可调伪随机置换安全性和 $\frac{l}{l+2}\cdot n$ 比特的强可调伪随机置换安全性. 第 3 节提出的改进的随机置换模型下的拓展镜像理论仍然考虑的是二变量镜像理论, 因此并不能直接适用, 需要提出基于多变量的拓展镜像系统超图理论. 当应用在 GCoTEM 的安全性证明中时, 需要将基于多变量的拓展镜像系统转化为上述改进的拓展镜像理论. 由于每个 l 变量的仿射等式都可以使用 $l/2$ 个二变量的仿射等式方程组来描述, 且对输出值引入更多的变量进行了截分, 这使得转化后等式方程组系统分析的过程稍微复杂. 这里我们将基于多变量的拓展镜像系统超图理论以及如何使用改进的拓展镜像理论证明 GCoTEM 方案确保了 $\frac{l}{l+1}\cdot n$ 比特的安全性作为一个开放性问题遗留下来以期进一步讨论与研究.

上述描述的超生日界安全的可调密码本原都是基于多个独立置换和独立密钥构造的. 在实际设计中, 应当尽可能地减少独立置换和密钥材料, 因此, 基于单个公开置换和单个密钥、具有最小结构、超生日界安全的可调密码本原设计更受欢迎.

假设 P 是一个公开随机置换, K 是一个 n 比特密钥, $t=(t_1,t_2)$ 是可调调柄且 $t_1\neq t_2$, $h': \mathcal{K}\times\Gamma\to\{0,1\}^{n-1}$ 是 ϵ_1-近乎均匀且 ϵ_2-AXU 泛哈希函数, 则基于单个置换和单个密钥的两个可调 Even-Mansour 密码实例的异或和构造的超生日界安全的可调伪随机函数 mSoTEM 定义为

$$y=\mathrm{mSoTEM}^{P,h'}_{K}(t,x)=P((x\oplus h'_K(t_1))||0)\oplus P((x\oplus h'_K(t_2))||1)\oplus h'_K(t_1)||0\oplus h'_K(t_2)||1.$$

类似于 SoTEM 的分析过程, mSoTEM 也是可证明超生日界安全的可调伪随机函数, 并且支持 $\frac{2n}{3}$ 比特的安全性. mSoTEM 的设计采用了域分离技术, 这使得输入并不是 n 比特长的明文, 而且对泛哈希的输出空间同样限制到 $n-1$ 比特长, 如何使用域保持技术设计基于单个公开置换和单个密钥、具有最小结构、超生日界安全的可调密码本原是未来重要的研究方向之一.

现有的密码方案或通信协议都是基于密码本原设计的, 因此可调密码本原可以广泛使用在如加密模式、消息认证码、认证加密以及相关的网络通信协议中 [29~37]. 除此之外, 多用户安全也颇受关注, 基于多用户安全的可调密码本原设计也是未来的研究方向之一 [38~40].

6　总结与展望

本文聚焦超生日界安全的可调密码本原设计与分析. 首先针对陈玉龙提出的随机置换模型下的拓展镜像理论限制了随机置换查询的差异性等问题, 对随机置换查询做了差异化改进, 同时引入置换查询交集非空的广阔空间, 给出了更一般性的适配拓展镜像理论解的上界. 然后, 从基于公共置换的可调 Even-Mansour 密码并级联结构出发, 设计了基于可调 Even-Mansour 密码实例的超生日界安全的可调伪随机函数和强可调伪随机置换. 基于新改进的拓展镜像理论证明了新设计的可调密码本原都是 $2n/3$ 比特紧致安全的. 最后, 讨论了超生日界安全的可调密码本原的设计与分析思路, 留下了推广多变量拓展镜像系统超图理论以及设计基于单个公开置换和单个密钥, 具有域保持和最小结构, 超生日界安全兼具多用户安全的可调密码本原开放性问题. 本文拓展了镜像理论和密码本原内涵, 对于构建可证明超生日界安全的对称密码方案具有重要的理论研究意义与实践指导价值.

参考文献

1 Wu W L, Feng D G, Zhang W T. Design and Analysis of Block Ciphers. 2nd ed. Beijing: Tsinghua University Press, 2009. 355–356 [吴文玲, 冯登国, 张文涛. 分组密码设计与分析 (第二版). 北京: 清华大学出版社, 2009. 355–356]

2 Luby M, Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. SIAM J Comput, 1988, 17: 373–386

3 Pieprzyk J. How to construct pseudorandom permutations from single pseudorandom functions. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, 1990. 140–150

4 Bellare M, Krovetz T, Rogaway P. Luby-Rackoff backwards: increasing security by making block ciphers non-invertible. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, 1998. 266–280

5 Lucks S. The sum of PRPs is a secure PRF. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, 2000. 470–484

6 Mennink B, Neves S. Encrypted davies-Meyer and its dual: towards optimal security using mirror theory. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2017. 556–583

7 Datta N, Dutta A, Nandi M, et al. Encrypt or decrypt? To make a single-key beyond birthday secure nonce-based MAC. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2018. 631–661

8 Gilboa S, Gueron S. The advantage of truncated permutations. Discrete Appl Math, 2021, 294: 214–223

9 Chen Y L, Lambooij E, Mennink B. How to build pseudorandom functions from public random permutations. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2019. 266–293

10 Dutta A, Nandi M, Talnikar S. Permutation based EDM: an inverse free BBB secure PRF. IACR Trans Symmetric Cryptol, 2021, 2021: 31–70

11 Chen S, Lampe R, Lee J, et al. Minimizing the two-round Even-Mansour cipher. J Cryptol, 2018, 31: 1064–1119

12 Chen S, Lampe R, Lee J, et al. Minimizing the two-round Even-Mansour cipher. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2014. 39–56

13 Patarin J. On linear systems of equations with distinct variables and small block size. In: Proceedings of International Conference on Information Security and Cryptology, 2005. 299–321

14 Patarin J. Introduction to mirror theory: analysis of systems of linear equalities and linear non equalities for cryptography. IACR Cryptol ePrint Arch, 2010, 2010: 287

15 Patarin J. Mirror theory and cryptography. Appl Algebra Eng Commun Comput, 2017, 28: 321–338

16 Nachef V, Patarin J, Volte E. Introduction to Mirror Theory. Berlin: Springer-Verlag, 2017. 203–221

17 Dutta A, Nandi M, Saha A. Proof of mirror theory for $\xi_{\max} = 2$. IEEE Trans Inform Theor, 2022, 68: 6218–6232

18 Datta N, Dutta A, Dutta K. Improved security bound of (E/D)WCDM. IACR Trans Symmetric Cryptol, 2021, 2021: 138–176

19 Chen Y L. A modular approach to the security analysis of two-permutation constructions. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2022. 379–409

20 Cogliati B, Dutta A, Nandi M, et al. Proof of mirror theory for a wide range of $\xi_{\max}$. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, 2023. 470–501

21 Rogaway P. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, 2004. 16–31

22 Mennink B. XPX: generalized tweakable Even-Mansour with improved security guarantees. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2016. 64–94

23 Granger R, Jovanovic P, Mennink B, et al. Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, 2016. 263–293

24 Cogliati B, Ethan J, Lallemand V, et al. CTET+: a beyond-birthday-bound secure tweakable enciphering scheme using a single pseudorandom permutation. IACR Trans Symmetric Cryptol, 2021, 2021: 1–35

25 Dutta A. Minimizing the two-round tweakable Even-Mansour cipher. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, 2020. 601–629

26 Bogdanov A, Knudsen L R, Leander G, et al. Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 45–62

27 Patarin J. The "coefficients H" technique. In: Proceedings of International Workshop on Selected Areas in Cryptography, 2008. 328–345

28 Cogliati B, Lampe R, Seurin Y. Tweaking Even-Mansour ciphers. In: Proceedings of Annual Cryptology Conference, Santa Barbara, 2015. 189–208

29 Cogliati B, Seurin Y. EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2016. 121–149

30 Dutta A, Jha A, Nandi M. Tight security analysis of EHtM MAC. IACR Trans Symmetric Cryptol, 2017, 3: 130–150

31 Chakraborti A, Nandi M, Talnikar S, et al. On the composition of single-keyed tweakable Even-Mansour for achieving BBB security. IACR Trans Symmetric Cryptol, 2020, 2020: 1–39

32 Choi W, Inoue A, Lee B, et al. Highly secure nonce-based MACs from the sum of tweakable block ciphers. IACR Trans Symmetric Cryptol, 2020, 2020: 39–70

33 Shen Y, Wang L, Gu D, et al. Revisiting the security of DbHtS MACs: beyond-birthday-bound in the multi-user setting. In: Proceedings of Annual International Cryptology Conference, 2021. 309–336

34 Chen Y L, Dutta A, Nandi M. Multi-user BBB security of public permutations based MAC. Cryptogr Commun, 2022, 14: 1145–1177

35 Furuya I, Kasahara H, Inoue A, et al. PMACrx: a vector-input MAC for high-dimensional vectors with BBB security. In: Proceedings of International Workshop on Security, Yokohama, 2023. 77–97

36 Naito Y. The multi-user security of MACs via universal hashing in the ideal cipher model. In: Proceedings of Cryptographers' Track at the RSA Conference, San Francisco, 2024. 51–77

37 Datta N, Dutta A, Nandi M, et al. Tight multi-user security bound of DbHtS. IACR Trans Symmetric Cryptol, 2023, 2023: 192–223

38 Naito Y, Sasaki Y, Sugawara T. The exact multi-user security of (tweakable) key alternating ciphers with a single permutation. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, 2024. 97–127

39 Chen Y L, Choi W, Lee C. Improved multi-user security using the squared-ratio method. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2023. 694–724

40 Cogliati B. Tweaking a block cipher: multi-user beyond-birthday-bound security in the standard model. Des Codes Cryptogr, 2018, 86: 2747–2763

Beyond-birthday-bound (BBB) secure tweakable cryptographic primitives based on tweakable Even-Mansour cipher instances

Ping ZHANG[1,2] & Yiyuan LUO[3*]

1. *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
2. *Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu 610225, China*
3. *School of Computer Science and Engineering, Huizhou University, Huizhou 516007, China*
* Corresponding author. E-mail: luoyy@hzu.edu.cn

Abstract In recent years, beyond-birthday-bound (BBB) secure cryptographic primitives have attracted much attention. As an extension of the traditional cryptographic primitive, tweakable cryptographic primitive also plays an important role in cryptographic algorithms or network security communication protocols. However, there are few BBB-secure designs. Therefore, this paper focuses on the design and analysis of BBB-secure tweakable cryptographic primitives. Starting from the tweakable Even-Mansour cipher based on the public permutation, the goal is to design the tweakable pseudo-random function (TPRF) and strong tweakable pseudo-random permutation (STPRP) based on the tweakable Even-Mansour cipher instances. Firstly, in view of the problems that the extended mirror theory under the random permutation model proposed by Chen Yulong restricts the difference of different random permutation queries and the intersection is empty, distinct queries are made to different random permutations and the intersection is non-empty extension, and the more generalized upper bound of the adapted extended mirror theory is given. Then, BBB-secure TPRF and STPRP are respectively constructed by the summation and cascade of two tweakable Even-Mansour cipher instances, and their provable security results are respectively given by our improved extended mirror theory. Finally, BBB-secure symmetric cryptographic primitives constructed by the summation and cascade of multiple tweakable Even-Mansour cipher instances and the multivariate-based mirror system hypergraph theory on which they depend, and the design ideas of single-permutation and single-key based BBB-secure symmetric cryptographic primitives with minimal structure and domain preserving are discussed. Our works enrich mirror theory and cryptographic primitives, and have important theoretical significance and practical guiding value for building a provably BBB-secure symmetric cryptographic scheme.

Keywords beyond-birthday-bound (BBB) security, tweakable cryptographic primitive, tweakable Even-Mansour cipher, mirror theory, random permutation model (RPM)