软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software [doi: 10.13328/j.cnki.jos.007092]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

标准模型下效率更高的身份基匹配加密*

陈 洁[1], 楚乔涵[1], 杜秋妍[1], 高 莹[2,3]

[1](华东师范大学 软件工程学院, 上海 200062)

[2](北京航空航天大学 网络空间安全学院, 北京 100191)

[3](中关村实验室, 北京 100191)

通信作者: 杜秋妍, E-mail: 52285902003@stu.ecnu.edu.cn

摘 要: 身份基匹配加密是一种新型的密码学原语, 允许接收者与发送者双方都可以指定对方的身份, 只有身份匹配时才可与之通信. 这项加密技术提供了一种非交互式的秘密握手协议以摆脱实时互动, 进一步提高参与者的隐私性. 在标准模型下基于 SXDH 假设, 提出素数阶群上的身份基匹配加密方案, 实现短参数, 降低解密时的配对次数, 是目前效率最高的身份基匹配加密方案. 此外, 还提出第 1 个标准模型下基于 SXDH 假设的等值策略的内积匹配加密方案. 技术路线如下, 首先构造合数阶群上的方案, 然后通过 DPVS 技术将方案模拟到素数阶群中, 并降低所需的对偶基维数, 进一步减小参数大小. 最后, 替换身份基匹配加密的第 1 层策略, 构造出等值策略的内积匹配加密方案.

关键词: 身份基匹配加密; 内积匹配加密; 对偶配对向量空间; SXDH 假设

中图法分类号: TP306

中文引用格式: 陈洁, 楚乔涵, 杜秋妍, 高莹. 标准模型下效率更高的身份基匹配加密. 软件学报. http://www.jos.org.cn/1000-9825/7092.htm

英文引用格式: Chen J, Chu QH, Du QY, Gao Y. More Efficient Identity-based Matchmaking Encryption under Standard Model. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7092.htm

More Efficient Identity-based Matchmaking Encryption under Standard Model

CHEN Jie[1], CHU Qiao-Han[1], DU Qiu-Yan[1], GAO Ying[2,3]

[1](Software Engineering Institute, East China Normal University, Shanghai 200062, China)

[2](School of Cyber Science and Technology, Beihang University, Beijing 100191, China)

[3](Zhongguancun Laboratory, Beijing 100191, China)

Abstract: Identity-based matchmaking encryption is a new cryptographic primitive that allows both the receiver and the sender to specify each other's identity and communicate with each other only when the identities match. Meanwhile, it provides a non-interactive secret handshake protocol to get rid of real-time interaction and further improve participant privacy. This study proposes an identity-based matchmaking encryption (IB-ME) scheme in prime-order groups under symmetric external Diffie-Hellman (SXDH) assumption under the standard model. Realizing short parameters and reducing the matchmaking times during decryption are the most efficient identity-based matchmaking encryption scheme. Additionally, this study also puts forward the first inner product with equality matchmaking encryption (IPE-ME) scheme under the SXDH assumption in the standard model. Technically, it first constructs two schemes in composite-order groups, then simulates them with dual pairing vector space (DPVS) into prime-order groups, and further reduces the parameter size by decreasing the required dimension of dual basis. Finally, for the proposed IPE-ME scheme, this study replaces the equality policy in the

* 基金项目: 国家自然科学基金 (61972156, 62372180); 国家自然科学基金 NSFC-ISF 合作项目 (61961146004); 国家重点研发计划 (2018YFA0704701); 上海市教育委员会科研创新计划 (2021-01-07-00-08-E00101); "数字丝路"可信智能软件国际联合实验室 (22510750100)
收稿时间: 2023-06-12; 修改时间: 2023-08-18; 采用时间: 2023-11-13; jos 在线出版时间: 2024-04-24

first layer of an IB-ME scheme with inner-product policy.

Key words: identity-based matchmaking encryption (IB-ME); inner-product matchmaking encryption; dual pairing vector spaces (DPVS); symmetric external Diffie-Hellman (SXDH)

1 引 言

● 匹配加密 (matchmaking encryption, ME)

匹配加密是 Ateniese 等人[1]引入的一个密码学原语. 匹配加密可以使得发送者和接收者双方都可以规定各自的策略, 只有满足策略的对象才能进行消息传输.

它的目的是制定一个非交互式的秘密握手协议[2]以摆脱实时互动, 并进一步提高参与者的隐私性. 除了非交互性和强隐私性, 在 Ateniese 等人[1]对匹配加密的定义中还具有真实性, 以此消除在匿名通信中的不可信问题.

具体来说, 匹配加密方案的工作原理如下: 可信中心分别用发送方属性 σ 和接收方属性 ρ 来生成相应的发送方密钥 ek_σ 和接收方密钥 dk_ρ, 并分别发送给他们. 当发送秘密信息时, 发送方需指定一个策略 $\mathbb{R}$, 并用 ek_σ 和 $\mathbb{R}$ 对信息进行加密, 只有属性 ρ 与策略 $\mathbb{R}$ 相匹配的接收方才有资格解密. 另一方面, 接收方也可以指定一个策略 $\mathbb{S}$, 并向可信中心进行 $\mathrm{dk}_\mathbb{S}$ 的问询, 这样就可以识别信息源.

基于匹配加密的功能, 它有很多实际应用. 在 Ateniese 等人[1]的文章中给出了两个例子. 一个例子是一个发送方可以指定接收方是居住在纽约的一名 FBI 特工, 而接收方也可以指定发送方是一名 CIA 特工. 如果解密失败, 不会泄露任何的隐私信息. 另一个例子是加密竞标: 竞标者可以向收集者发送用他们选择的条件来加密的标书, 而收集者可以打开满足特定要求的标书. 同样的, 如果解密失败, 收集者既不会知晓原因也不能得到实际标书中的信息. Ateniese 等人[1]还实现了附带匹配加密下的 Tor 隐藏服务与隐私保护公告板的结合, 其中匹配加密可以允许各方收集来自于匿名的真实来源的信息.

● 身份基匹配加密 (identity-based matchmaking encryption, IB-ME)

身份基匹配加密是一种在策略 $\mathbb{R}$ 和 $\mathbb{S}$ 一致的特定情况下的匹配加密, 即策略被单一身份 *rcv* 和 *snd* 分别取代. IB-ME 的一个值得注意的地方是, 与一般的 ME 不同, 在 IB-ME 中, 接收方不需要对 $\mathbb{S}$ (即 *snd*) 进行 $\mathrm{dk}_\mathbb{S}$ 的问询, 从而免除了生成 $\mathrm{dk}_\mathbb{S}$ 的算法. 尽管 IB-ME 是 ME 的一个特例, 但只要允许策略放宽到相等, 它也是适用的. 例如 Ateniese 等人[1]说明的, 在匿名但可靠的通讯场景中已经存在着对于 IB-ME 的应用.

目前已有一系列的 IB-ME 构造. Ateniese 等人[1]在随机预言机模型下基于双线性 Diffie-Hellman (bilinear Diffie-Hellman, BDH) 假设构造了第 1 个 IB-ME 方案. 他们接下来 Francati 等人[3]将 IB-ME 改进为标准模型, 但他们的方案建立在非标准的 q-type 假设上. 随后, Chen 等人[4]提出了在标准模型下基于标准 SXDH 假设的 IB-ME 方案.

● 等值策略的内积匹配加密 (inner-product with equality matchmaking encryption, IPE-ME)

IPE-ME 是 IB-ME 的升级版, 即策略 $\mathbb{R}$ 由等值升级为内积, 扩大发送方的权限. 例如, 在匿名且可靠的通讯中, 发送方可以指定他选择的策略为一个权重向量, 这样将得到接收方精确的目标分数, 进一步地, 发送方可以指定一个以上的接收方, 其属性与发送方的策略匹配. 而接收方可以像在 IB-ME 中一样通过 σ-*snd* 对的等值策略来检验信息源.

1.1 研究现状

首个 ME 的一般方案是由 Ateniese 等人[1]提出的, 这个方案是由功能加密 (functional encryption, FE)、签名及非交互式零知识证明 (non-interactive zero-knowledge proofs, NIZK) 以黑箱的方法构造而成的. Ateniese 等人也提出了一个基于 BDH 假设的安全 IB-ME 方案, 其结构比上述 ME 的一般方案更直接, 但是在随机预言机模型下构造的. 然为了改进这个方面, Francati 等人[3]提出了一个不需要随机预言机就可以达到隐私性的 IB-ME 方案, 这个方案由可重复使用的计算提取器, 签名及 NIZK 构造的, 但这个方案基于复杂的 q-type 假设. 最近, Chen 等人[4]提出了第 1 个标准模型下基于标准假设的 IB-ME 方案. 他们的方案基于一个双层 IBE 结构, 直接从基于 SXDH 假

设的素数阶群匿名身份基加密 (identity-based encryption, IBE) 方案衍生出来的, 本文也基于这种结构完成方案的构造.

根据 Ateniese 等人[1]的工作, Xu 等人[5]将 ME 扩展到一个新的原语, 称之为属性基匹配加密 (matchmaking attribute-based encryption, MABE), 以提供安全的细粒度双边访问控制, 并且保障数据的真实性. 但是在 ME 和 MABE 中数据解密过程开销很高, 这限制了它们在资源有限的物联网设备中的应用. 为了解决这个问题, Xu 等人[6]随后引入了一个新的原语, 称之为轻量级匹配加密 (lightweight matchmaking encryption, LME), 并给出了具体结构. 聂旭云等人[7]基于属性基匹配加密并结合穿刺加密技术, 构造了具有前向安全性的属性基匹配加密方案.

上述方案是匹配加密提出以来具体的方案构造, 扩展了匹配加密的应用场景, 但效率问题仍待解决.

1.2 研究问题

目前的匹配加密方案较为单一, 现在仅有身份基和属性基匹配加密. 可应用的场景较少. 而且目前的匹配加密方案效率较低, 影响实用性, 即在效率上尚有改进的空间. 因此, 本文从以下两方面进行了改进.

● 进一步提高效率, 从而提升 IB-ME 方案的可应用性.

本文从降低参数长度以及减少配对次数两个方向分别改善方案效率.

● 研究设计新的匹配加密构造, 丰富应用场景.

本文构造了等值策略的身份基匹配加密 (IPE-ME) 方案, 满足更复杂的匹配策略.

1.3 结果和讨论

本文致力于提高现有的 IB-ME 方案的效率, 主要贡献如下.

● 遵循在标准模型下基于 SXDH 假设的非对称素数阶群上双层匿名 IBE 构造, 提出了两种 IB-ME 方案, 相比于 Chen 等人[4]的方案更加高效. 具体来讲, 第 1 个素数阶方案比起 Chen 等人的方案具有更短的参数, 但多一次解密配对, 也比第 2 种方案多 3 次解密配对. 表 1 有详细的比较, 其中 $|\cdot|$ 表示群中一个群元素的大小.

表 1　现有的标准模型下基于标准假设的 IB-ME 方案性能比较

方案	|mpk|	|ek|	|dk|	|ct|	配对
CLWW22[4]	$16\|G\|+2\|G_T\|$	$8\|G\|$	$16\|H\|+\|G_T\|$	$8\|G\|+\|G_T\|$	8
Π_{C1}	$15\|G\|+\|G_T\|$	$6\|G\|$	$9\|H\|$	$9\|G\|+\|G_T\|$	9
Π_{C2}	$15\|G\|+\|G_T\|$	$9\|G\|$	$9\|H\|$	$9\|G\|+\|G_T\|$	6

● 构造了两个在标准模型下基于子群判定 (subgroup decision, SD) 假设下的合数阶群上的 IB-ME 方案, 作为两种素数阶群上的方案的准备工作. 从技术上讲, 素数阶群的版本是通过对偶配对空间向量 (dual pairing vector spaces, DPVS)[8,9]的方法由合数阶群模拟得到的.

● 在标准模型下基于 SXDH 假设构造了非对称素数阶群上的 IPE-ME 方案. 此方案由 Chen 等人[4]的 IB-ME 方案改进得到, 并使用了 Chen 等人[10]的工作中将 IBE 扩展到弱属性隐藏内积加密 (inner-product encryption, IPE) 的方法[9,11−15].

2 技术挑战与总览

● IB-ME. 受到 Chen 等人的双层结构[4]启发, 观察到可以将他们的匿名 IBE[16]替换成一般 ABE 框架[17]的构造, 这种构造基于谓词编码[15]. 替换后的 IBE 构造如下:

$$\begin{cases} \mathrm{mpk} = (g, g^{w_1}, g^{w_2}, h, g_T^{\alpha}) \\ \mathrm{msk} = (w_1, w_2, \alpha) \\ \mathrm{ct} = (C_0 = g^{s}, C_1 = g^{sw_1} g^{id \cdot sw_2}, C_2 = g_T^{s\alpha} \cdot m) \\ \mathrm{sk} = (K_0 = h^{r}, K_1 = h^{\alpha} \cdot h^{rw_1} h^{id \cdot rw_2}) \\ m = C_2 / (e(C_0, K_1) / e(C_1, K_0)) \end{cases} .$$

然后需要将上述 IBE 的两个实例有效地结合起来以获得 IB-ME. 第 1 个难点在于不可能直接通过结合上述 IBE 的两个实例在素数阶群中构造 IB-ME 方案, 原因是两个实例的随机性是独立的, 这导致在解密阶段中有些项无法消去. 也就是说, 在解密阶段会存在着类似 $g_T^{sw_i r'}/g_T^{s' w_i r}$ 这样的项, 原因是两个 IBE 实例没有正交性, 不像是在 Chen 等人[16]的方案中的 IBE 完全满足正交性.

为了使得两个实例正交, 一个自然的想法是首先将素数阶群转化为合数阶群. 对于每个实例都使用不同的子群, 这样立即得到了两个不同的 IB-ME 构造. 其中一个方案比另一个参数更长, 但所需的解密配对次数少. 而其中参数短的方案的密钥由一个群元素组成, 但所需的解密配对次数多.

而目标是在素数阶群上构造 IB-ME 方案, 所以下一步是将合数阶群的版本模拟到素数阶群上, 这里要使用 DPVS 技术. 模拟将会增加参数大小, 因为合数阶群版本中每一个的群元素需要素数阶群版本中 4 个群元素来模拟. 而且最终的构造几乎与 Chen 等人[4]的一样.

突破的关键点在于 IB-ME 的隐私性只需要考虑 *rcv*–ρ 对, 因为 σ-*snd* 对不需要向可信中心问询并且 IB-ME 中的密文可以通过 *rcv*–ρ 对隐藏 σ. 所以安全分析无需二维对偶基只需要一维. 这意味着只需要 3 个群元素就可以模拟合数阶版本中的一个群元素. 另外, 可以观察到对于第 2 层的 IBE 中 g_T^{α} 实际上是不必须的, 因为第 2 层的作用是签名, 而对于签名, g_T^{α} 可以设为 $g_T^0=[1]_T$. 因此, mpk 和 dk 中可以分别减少 1 个群元素. 综上所述, 就可以得到比 Chen 等人[4]的更加高效的素数阶群上的 IB-ME 方案.

● IPE-ME. 遵循 Chen 等人[10]将匿名 IBE 扩展到弱属性隐藏 IPE 的方法, 进一步将他们的 IB-ME 方案中 *rcv*–ρ 的等值策略替换成内积策略, 就得到了 IPE-ME 方案. 方案也随着上述结论而改进. 他们的 IB-ME 方案之所以会很容易地改进成 IPE-ME 方案, 是因为在将 IBE 扩展为 IPE 时 Chen 等人的 IBE 方案结构不需要将指数中的属性显式相乘, 因此可以依照 IB-ME 的结构来构造 IPE-ME.

3 预备知识

3.1 记　号

$\leftarrow_R$ 表示随机抽样, PPT 表示概率多项式时间, $negl(\lambda)$ 表示安全参数为 λ 的可忽略函数, 黑体大写字母表示矩阵, 黑体小写字母表示向量, $\langle\cdot,\cdot\rangle$ 表示内积.

3.2 假　设

定义 1. SD 假设 (子群判定假设, subgroup decision assumption)[18,19]. 令 $e: G\times H\to G_T$ 为群生成元 $\mathcal{G}(\lambda)$ 生成的非退化的非对称双线性群映射, G,H 和 G_T 的阶数为 $N=p_1p_2p_3$, 其中 p_1,p_2,p_3 是素数. 对于 $i,j\in[3], i\neq j$, 用 G_{p_i} 表示阶数为 p_i 的相应的子群, 用 $G_{p_ip_j}$ 表示阶数为 p_ip_j 的相应的子群. 用 g_i 表示 G_{p_i} 的生成元, 用 g_{ij} 来表示 $G_{p_ip_j}$ 的生成元 (任意选择). 对于群 H 也相应处理.

SD 假设: 给定 $\mathbb{G}=(N,G,H,G_T,e),(g_1,g_2,g_3)$ 以及 (h_1,h_{12},h_3), 对于任何 PPT 敌手 $\mathcal{A}$, 区分 $T_1\leftarrow_R G_{p_1}$ 与 $T_2\leftarrow_R G_{p_1p_2}$ 是困难的.

即 $\mathrm{Adv}_{\mathcal{A}}^{SD}(\lambda)=|\Pr[\mathcal{A}(\mathbb{G},g_1,g_2,g_3,h_1,h_{12},h_3,T_1)1-\Pr[\mathcal{A}(\mathbb{G},g_1,g_2,g_3,h_1,h_{12},h_3,T_2)=1]|\leqslant negl(\lambda)$.

注 1. 当下标变换时假设仍成立.

注 2. 当把 g_{12} 写成 $g_{12}=g_1^{\gamma_1}\cdot g_2^{\gamma_2}$ 时, γ_1,γ_2 应该被限制在 $\gamma_1\leftarrow_R\mathbb{Z}_N/\{k_1\cdot p_1\}_{k_1\in[p_2p_3]}$, $\gamma_2\leftarrow_R\mathbb{Z}_N/\{k_2\cdot p_2\}_{k_2\in[p_1p_3]}$. 这将导致一个可以忽略不计的差异 $\frac{1}{p_1}+\frac{1}{p_2}$. 为了简单起见, 下面将省略这个可以忽略不计的概率, 并简单地写成 $g_{12}=g_1^{\gamma_1}\cdot g_2^{\gamma_2}$, 其中 $\gamma_1,\gamma_2\leftarrow_R\mathbb{Z}_N$.

定义 2. DS 假设 (判定子空间假设, decisional subspace assumption). 令 $e: G\times H\to G_T$ 为群生成元 $\mathcal{G}(\lambda)$ 生成的非退化的非对称双线性群映射, G,H 和 G_T 的阶数为 $N=p$. 令 $(\mathbb{D}=(\mathbf{d}_1,\ldots,\mathbf{d}_n),\mathbb{D}^*=(\mathbf{d}_1^*,\ldots,\mathbf{d}_n^*))\leftarrow_R Dual\left(\mathbb{Z}_p^n\right)$ 为两个随机的对偶正交基, 取 $\tau_1,\tau_2,\mu_1,\mu_2\leftarrow_R\mathbb{Z}_p$.

G 上的 DS 假设: 给定 $\mathbb{G}=(p,G,H,G_T,e,g,h),\left(h^{\mathbf{d}_1},h^{\mathbf{d}_2},\ldots,h^{\mathbf{d}_\eta},h^{\mathbf{d}_{\eta+1}^*},\ldots,h^{\mathbf{d}_n^*}\right),(g^{\mathbf{d}_1},\ldots,g^{\mathbf{d}_n})$, $(h^{\mu_1\mathbf{d}_1^*+\mu_2\mathbf{d}_{k+1}^*},h^{\mu_1\mathbf{d}_2^*+\mu_2\mathbf{d}_{k+2}^*},\ldots,$

$h^{\mu_1\mathbf{d}_k^*+\mu_2\mathbf{d}_{2n}^*}$) 和$\mu_2$，对于任何 PPT 敌手$\mathcal{A}$，区分$(V_1=g^{\tau_1\mathbf{d}_1},\ldots,V_k=g^{\tau_1\mathbf{d}_k})$和$(W_1=g^{\tau_1\mathbf{d}_1+\tau_2\mathbf{d}_{k+1}},\ldots,W_k=g^{\tau_1\mathbf{d}_k+\tau_2\mathbf{d}_{2k}})$是困难的.

即 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DS1}}(\lambda)=|\Pr[\mathcal{A}(\mathcal{D},(V_1,\ldots,V_k))=1]-\Pr[\mathcal{A}(\mathcal{D},(W_1,\ldots,W_k))=1]|\leqslant negl(\lambda)$.

其中 $\mathcal{D}=\left(\mathbb{G},\left(h^{\mathbf{d}_1^*},h^{\mathbf{d}_2^*},\ldots,h^{\mathbf{d}_\eta^*},h^{\mathbf{d}_{\eta+1}^*},\ldots,h^{\mathbf{d}_n^*}\right),(g^{\mathbf{d}_1},\ldots,g^{\mathbf{d}_n}),(h^{\mu_1\mathbf{d}_1^*+\mu_2\mathbf{d}_{k+1}^*},h^{\mu_1\mathbf{d}_2^*+\mu_2\mathbf{d}_{k+2}^*},\ldots,h^{\mu_1\mathbf{d}_k^*+\mu_2\mathbf{d}_{2n}^*}),\mu_2\right)$.

注 3. H 上的 DS 假设几乎与 G 上的 DS 假设相同.

定义 3. DDH1 假设 (G_1 的判定 Diffie-Hellman 假设, decisional Diffie-Hellman assumption in G_1). 令 $e:G_1\times G_2\to G_T$ 为由群生成元$\mathcal{G}(\lambda)$生成的非退化的双线性群映射, 其中 G_1,G_2 和 G_T 的阶数为 p. 用 g_i 表示 G_i 的生成元. 取 $a,b,c\leftarrow_R\mathbb{Z}_p$.

DDH1 假设: 给定 $\mathbb{G}=(p,G_1,G_2,G_T,e,g_1,g_2),g_1^a,g_1^b$, 对于任何 PPT 敌手 $\mathcal{A}$, 区分 g_1^{ab} 和 g_1^{ab+c} 是困难的.

即 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DDH1}}(\lambda)=\left|\Pr[\mathcal{A}((\mathbb{G},g_1^a,g_1^b),g_1^{ab})]-\Pr[\mathcal{A}((\mathbb{G},g_1^a,g_1^b),g_1^{ab+c})\right|\leqslant negl(\lambda)$.

注 4. DDH2 假设即是将 DDH1 假设中的群 G_1 置换为群 G_2.

定义 4. SXDH 假设 (判定子空间假设, decisional subspace assumption). SXDH 假设成立, 如果 DDH 假设在群 G_1 和 G_2 都成立.

注 5. DS 假设可以分别被紧规约到相应群上的 SXDH 假设.

3.3 身份基匹配加密 (IB-ME)

本节涉及的定义主要基于 Ateniese 等人[1]的工作, 提取其文章中 IB-ME 的算法框架和安全性定义, 并省略了具体的构造.

3.3.1 语 法

一个 IB-ME 由以下的概率时间算法组成, Dec 算法是确定性的, 其他所有算法都是概率性的.

- 初始化 $\mathrm{Setup}(\lambda)\to(\mathrm{mpk},\mathrm{msk})$: 输入安全参数 λ，可信中心输出公开主公钥 mpk 和保存主私钥 msk.
- 生成加密密钥: 输入 mpk，msk 和身份 σ, 可信中心为发送方输出与身份 σ 相关的加密私钥 ek_σ.
- 生成解密密钥 $\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},\rho)\to\mathrm{dk}_\rho$: 输入 mpk，msk 和身份 ρ, 可信中心为接收方输出与身份 ρ 相关的解密密钥 dk_ρ.
- 加密 $\mathrm{Enc}(\mathrm{mpk},\mathrm{ek}_\sigma,rcv,m)\to\mathrm{ct}$: 发送方输入 mpk，$\mathrm{ek}_\sigma$，身份 rcv 和消息明文 m, 通过加密算法输出密文 ct.
- 解密 $\mathrm{Dec}(\mathrm{mpk},\mathrm{dk}_\rho,snd,\mathrm{ct})=m$: 接收方输入 mpk，$\mathrm{dk}_\rho$，身份 snd 和 ct, 输出解密算法 m 或者 $\perp$.

定义 5. IB-ME 的正确性. 一个 IB-ME 方案是正确的, 如果当 $\sigma=snd$ 和 $\rho=rcv$ 时, 满足:

$$\Pr\left[\mathrm{Dec}=m\;\middle|\;\begin{array}{l}\mathrm{mpk},\mathrm{msk}\leftarrow\mathrm{Setup}(\lambda)\\ \mathrm{ek}_\sigma\leftarrow\mathrm{SKGen}(\mathrm{mpk},\mathrm{msk},\sigma)\\ \mathrm{dk}_\rho\leftarrow\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},\sigma)\\ \mathrm{ct}\leftarrow\mathrm{Enc}(\mathrm{mpk},\mathrm{ek}_\sigma,rcv,m)\end{array}\right]\geqslant 1-negl(\lambda),$$

否则满足:

$$\Pr\left[\mathrm{Dec}=\perp\;\middle|\;\begin{array}{l}\mathrm{mpk},\mathrm{msk}\leftarrow\mathrm{Setup}(\lambda)\\ \mathrm{ek}_\sigma\leftarrow\mathrm{SKGen}(\mathrm{mpk},\mathrm{msk},\sigma)\\ \mathrm{dk}_\rho\leftarrow\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},\sigma)\\ \mathrm{ct}\leftarrow\mathrm{Enc}(\mathrm{mpk},\mathrm{ek}_\sigma,rcv,m)\end{array}\right]\geqslant 1-negl(\lambda).$$

3.3.2 安全性

定义 6. IB-ME 的安全性. 一个 IB-ME 方案 Π 满足安全性, 如果这个方案满足隐私性和真实性.

定义 7. IB-ME 的隐私性. 一个 IB-ME 方案 Π 满足隐私性, 如果对于任何有效 PPT 敌手 $\mathcal{A}$, 都有:

$$\left|\Pr\left[\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Priv}}(\lambda)=1\right]-\frac{1}{2}\right|\leqslant negl(\lambda),$$

其中, $\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Priv}}(\lambda)$ 的定义在图 1 中. 敌手 $\mathcal{A}$ 被称为有效的, 如果 $\forall\rho\in\mathcal{Q}_{O_2}$ 都满足下述不变性:

$$\rho\neq rcv_0\wedge\rho\neq rcv_1\left(\text{不匹配条件}\right).$$

定义 8. IB-ME 的真实性. 一个 IB-ME 方案 Π 满足真实性, 如果对于任何 PPT 敌手 $\mathcal{A}$ 都满足:

$$\Pr\left[\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Auth}}(\lambda)=1\right]\leqslant negl(\lambda),$$

其中, $\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Auth}}(\lambda)$ 的定义在图 1 中.

$\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Priv}}(\lambda)$	$\mathrm{Game}_{\Pi,\mathcal{A}}^{\text{IB-Auth}}(\lambda)$
$(\mathrm{mpk},\mathrm{msk})\leftarrow_{\mathrm{R}}\mathrm{Setup}(\lambda)$	$(\mathrm{mpk},\mathrm{msk})\leftarrow_{\mathrm{R}}\mathrm{Setup}(\lambda)$
$(m_0,m_1,rcv_0,rcv_1,\sigma_0,\sigma_1,st)\leftarrow_{\mathrm{R}}\mathcal{A}_1^{\mathcal{O}_1,\mathcal{O}_2}(\lambda,\mathrm{mpk})$	$(\mathrm{ct},\rho,snd)\leftarrow_{\mathrm{R}}\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}(\lambda,\mathrm{mpk})$
$\beta\leftarrow_{\mathrm{R}}\{0,1\}$	$\mathrm{dk}_\rho\leftarrow\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},\rho)$
$\mathrm{ek}_{\sigma_\beta}\leftarrow\mathrm{SKGen}(\mathrm{mpk},\mathrm{msk},\sigma_\beta)$	$m=\mathrm{Dec}(\mathrm{dk}_\rho,snd,\mathrm{ct})$
$\mathrm{ct}_\beta\leftarrow\mathrm{Enc}(\mathrm{ek}_{\sigma_\beta},rcv_\beta,m_\beta)$	当$\forall\sigma\in\mathcal{Q}_{\mathcal{O}_1}$:
$\beta'\leftarrow\mathcal{A}_2^{\mathcal{O}_1,\mathcal{O}_2}(\lambda,\mathrm{ct}_\beta,\mathrm{st})$	$(\sigma\neq snd)\wedge(\rho\notin\mathcal{Q}_{\mathcal{O}_2})\wedge(m\neq\perp)$返回 1
当$(\beta'=\beta)$返回 1; 否则返回 0	否则返回 0

图 1　IB-ME 的隐私性和安全性游戏 (预言机 O_1 和 O_2 由 $\mathrm{SKGen}(\mathrm{mpk},\mathrm{msk},\cdot)$ 和 $\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},\cdot)$ 实现)

3.4 等值策略的内积匹配加密

3.4.1 语　法

IPE-ME 和 IB-ME 的语法基本相同, 只有 RKGen 算法和 Enc 算法有如下修改.

● 生成解密密钥 $\mathrm{RKGen}(\mathrm{mpk},\mathrm{msk},v)$: 输入主公钥 mpk, 主私钥 msk, 属性 v, 可信中心为接收方输出关于 v 的解密密钥 dk_v.

● 加密 $\mathrm{Enc}(\mathrm{mpk},\mathrm{ek}_\sigma,\mathbf{x},m)$: 发送方输入主公钥 mpk, 加密密钥 ek_σ, 内积策略 $\mathbf{x}$ 和明文 m, 由此算法输出与 σ 和 $\mathbf{x}$ 相关的密文 ct.

3.4.2 安全性

IPE-ME 的安全性几乎与 IB-ME 一致, 除了隐私性, 在 IPE-ME 中敌手 $\mathcal{A}$ 攻击 $(m_0,m_1,\mathbf{x}_0,\mathbf{x}_1,\sigma_0,\sigma_1)$, 并且不匹配的条件改为 $\langle v,\mathbf{x}_0\rangle\neq 0\wedge\langle v,\mathbf{x}_1\rangle\neq 0$ (不匹配条件).

4 合数阶群上的 IB-ME

本节提出了两种在非对称合数阶群上 IB-ME 方案, 这两种方案基于不同的代数结构. 在第 4.1 节中提出了第 1 种方案作为预热, 然后在第 4.3 节中提出了更短的但需要更多的解密配对的方案. 方案中群的阶数是 3 个素数的积, 这是由于本文的 IB-ME 实际上是由两层匿名 IBE 组成的, 其中在实际结构中每层需要两个子群, 而在理想结构中需要一个.

4.1 预热: 构造 Π_{C1}

● 初始化 $\mathrm{Setup}(\lambda)$: 运行群生成元 $\mathbb{G}=(N=p_1p_2p_3,G,H,G_T,e,g,h)\leftarrow\mathcal{G}(\lambda)$, 可信中心输出 $\mathrm{pp}=\mathbb{G}$. 随机抽取 $w_1,w_2,w_3,w_4,\alpha\leftarrow_R\mathbb{Z}_N$, 然后输出 $\mathrm{mpk}=(g_1,g_1^{w_1},g_1^{w_2},g_1^{w_3},g_1^{w_4},e(g_1,h_1)^\alpha)$ 并公开, 储存 $\mathrm{msk}=(h_1,h_3,g_3,w_1,w_2,w_3,w_4,h_1^\alpha)$.

● 生成加密密钥 $\mathrm{SKGen}(\mathrm{pp},\mathrm{msk},\sigma)$: 取 $s_2\leftarrow_R\mathbb{Z}_N$, 然后输出:

$$\mathrm{ek}_\sigma=(K_0^2=g_3^{s_2},K_1^2=g_3^{s_2w_1}g_3^{s_2w_4\sigma},K_2^2=g_3^{s_2w_3}).$$

● 生成解密密钥 $\mathrm{RKGen}(\mathrm{pp},\mathrm{msk},\rho)$: 取 $r_1,r_2\leftarrow_R\mathbb{Z}_N$, 然后输出:

$$\mathrm{dk}_\rho=(K_0^1=h_1^{r_1}\cdot h_3^{r_2},K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^\alpha\cdot h_3^{r_2w_1},K_2^1=h_1^{r_1w_3}\cdot h_3^{r_2w_3}h_3^{r_2w_4}).$$

● 加密 $\mathrm{Enc}(\mathrm{pp},\mathrm{mpk},\mathrm{ek}_\sigma,rcv,m)$: 随机抽取 $s_1\leftarrow_R\mathbb{Z}_N$, 然后输出:

$$\mathrm{ct}=(C_0=g_1^{s_1}\cdot K_0^2,C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv}\cdot K_1^2,C_2=g_1^{s_1w_3}\cdot K_2^2,C_3=e(g_1,h_1^\alpha)^{s_1}\cdot m).$$

● 解密 $\mathrm{Dec}(\mathrm{pp},\mathrm{dk}_\rho,snd,\mathrm{ct})$: 计算 $m=C_3/(e(C_0,K_1^1)\cdot e(C_0,(K_2^1)^{snd})/e(C_1,K_0^1)\cdot e(C_2^{snd},K_0^1))$, 并输出.

正确性:

$$\begin{aligned}
&e(C_0,K_1^1)\cdot e(C_0,(K_2^1)^{snd})/e(C_1,K_0^1)\cdot e((C_2)^{snd},K_0^1)\\
&\quad=e(g_1^{(s_1)}\cdot g_3^{(s_2)},h_1^{(r_1w_1)}h_1^{(r_1w_2\cdot\rho)}h_1^{\alpha}\cdot h_3^{(r_2w_1)})\cdot e(g_1^{(s_1)}\cdot g_3^{(s_2)},h_1^{(r_1w_3snd)}\cdot h_3^{(r_2w_4snd)}h_3^{(r_2w_3snd)})\\
&\qquad/e(g_1^{(s_1w_1)}g_1^{(s_1w_2rcv)}\cdot g_3^{(s_2w_1)}g_3^{(s_2w_4\sigma)},h_1^{(r_1)}\cdot h_3^{(r_2)})\cdot e(g_1^{(s_1w_3snd)}\cdot g_3^{(s_2w_3snd)},h_1^{(r_1)}\cdot h_3^{(r_2)})\\
&\quad=e(g_1^{(s_1)},h_1^{(r_1w_1)}h_1^{(r_1w_2\,\rho)}h_1^{\alpha})\cdot e(g_3^{(s_2)},h_3^{(r_2w_1)})\cdot e(g_1^{(s_1)},h_1^{(r_1w_3snd)})\cdot e(g_3^{(s_2)},h_3^{(r_2w_4snd)})\cdot e(g_3^{(s_2)},h_3^{(r_2w_3snd)})\\
&\qquad/e(g_1^{(s_1w_1)}g_1^{(s_1w_2rcv)},h_1^{(r_1)})\cdot e(g_3^{(s_2w_1)}g_3^{(s_2w_4\,\sigma)},h_3^{(r_2)})\cdot e(g_1^{(s_1w_3snd)},h_1^{(r_1)})\cdot e(g_3^{(s_2w_3snd)},h_3^{(r_2)})\\
&\quad=e(g_1,h_1)^{\alpha s_1}.
\end{aligned}$$

4.2 安全性分析

根据定义 4, 若 IB-ME 方案 Π_{C1} 满足安全性, 则满足隐私性和真实性, 下文将分别分析.

4.2.1 隐私性证明

为了证明隐私性, 这里采用双系统加密方法[19,20], 即借助一个游戏序列, 将原始的安全性模型逐步近似到一个完全安全的安全性模型中, 以完成证明.

因此整个证明过程中, 除原始安全性模型使用的密钥和密文 (下文中称为正常型), 还要涉及一些辅助性的密文和密钥分布 (下文中称为半功能型), 具体的定义在定理 1 的证明中.

令 D 表示每次安全游戏中问询解密密钥 dk 次数的上界. 具体的游戏序列如下.

- $\mathrm{Game}_{\mathrm{real}}$: 方案 Π_{C1} 原始的安全性模型, 其中的使用的都是正常型.
- Game_1 : Game_1 中密文 ct 变为半功能型, 其余与 $\mathrm{Game}_{\mathrm{real}}$ 相同.
- $\mathrm{Game}_{2,j,n}$ ($j\in[D],n\in[3]$): $\mathrm{Game}_{2,j,n}$ 与 Game_1 的差别仅在于回应的解密密钥类型不同. $\mathrm{Game}_{2,j,n}$ 中敌手问询的前 $j-1$ 次解密密钥, 挑战者回应的解密密钥 dk_{ρ_v} 是半功能 3 型; 后 $D-j$ 次问询回应的 dk_{ρ_v} 是正常型; 而第 j 次问询回应的解密密钥 dk_{ρ_v} 随 n 变化, $\mathrm{Game}_{2,j,0}$ 中回应正常型, $\mathrm{Game}_{2,j,1}$ 中回应半功能 1 型, $\mathrm{Game}_{2,j,2}$ 中回应半功能 2 型, $\mathrm{Game}_{2,j,3}$ 中回应半功能 3 型.
- $\mathrm{Game}_{\mathrm{final}}$: 将 $(m_\beta,rcv_\beta,\sigma_\beta)$ 换成了 (m_R,rcv_R,σ_R) , 其中 $m_R\leftarrow_R G_T$ 且 $rcv_R,\sigma_R\leftarrow_R\mathbb{Z}_N$.

注 6. $\mathrm{Game}_{2,0,0}$ 就是 Game_1 .

注 7. $\mathrm{Game}_{2,j,0}$ 近似到 $\mathrm{Game}_{2,j,3}$ 的过程中实现了第 j 次回应的解密密钥由正常型逐步变化为半功能 3 型.

注 8. $\mathrm{Game}_{\mathrm{final}}$ 是完全安全的, 即 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{final}}}=0$, 因为 (m_R,rcv_R,σ_R) 是随机的.

为了完成游戏序列的过渡并实现 $\mathrm{Game}_{\mathrm{final}}$ 完全安全, 需要将原本能够解密的解密密钥 dk_{ρ_v} 与密文 ct (称为正常型的 dk_{ρ_v} 和 ct), 逐步过渡到无法实现解密的半功能 3 型解密密钥 dk_{ρ_v} 与半功能 1 型密文 ct .

因此所有 $\mathrm{ek}_\sigma,\mathrm{dk}_\rho$ 和 ct 的形式被设计成以下种类:

- ek_σ 的形式: $\begin{cases}K_0^2=g_3^{s_2}\\ K_1^2=g_3^{s_2w_1}g_3^{s_2w_4\sigma}\\ K_2^2=g_3^{s_2w_3}\end{cases}$.
- dk_ρ 的 4 种形式:

① 正常型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_3^{r_2}\\ K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_3^{r_2w_1}\\ K_2^1=h_1^{r_1w_3}\cdot h_3^{r_2w_4}h_3^{r_2w_3}\end{cases}$.

② 半功能 1 型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_2^{r'}\cdot h_3^{r_2}\\ K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho}\cdot h_3^{r_2w_1}\\ K_2^1=h_1^{r_1w_3}\cdot h_2^{r'w_3}\cdot h_3^{r_2w_4}h_3^{r_2w_3}\end{cases}$, 其中, $r'\leftarrow_R\mathbb{Z}_N$.

③ 半功能 2 型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_2^{r'}\cdot h_3^{r_2}\\ K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho}h_2^{\alpha'}\cdot h_3^{r_2w_1}\\ K_2^1=h_1^{r_1w_3}\cdot h_2^{r'w_3}\cdot h_3^{r_2w_4}h_3^{r_2w_3}\end{cases}$, 其中, $r',\alpha'\leftarrow_R\mathbb{Z}_N$.

④ 半功能 3 型 $\begin{cases} K_0^1 = h_1^{r_1} \cdot h_3^{r_2} \\ K_1^1 = h_1^{r_1 w_1} h_1^{r_1 w_2 \rho} h_1^{\alpha} \cdot h_2^{\alpha'} \cdot h_3^{r_2 w_1} \\ K_2^1 = h_1^{r_1 w_3} \cdot h_3^{r_2 w_4} h_3^{r_2 w_3} \end{cases}$, 其中, $\alpha' \leftarrow_R \mathbb{Z}_N$.

● ct 的 2 种形式.

① 正常型 $\begin{cases} C_0 = g_1^{s_1} \cdot g_3^{s_2} \\ C_1 = g_1^{s_1 w_1} g_1^{s_1 w_2 rcv} \cdot g_3^{s_2 w_1} g_3^{s_2 w_4 \sigma} \\ C_2 = g_1^{s_1 w_3} \cdot g_3^{s_2 w_3} \\ C_3 = e(g_1, h_1)^{\alpha s_1} \cdot m \end{cases}$.

② 半功能 1 型 $\begin{cases} C_0 = g_1^{s_1} \cdot g_2^{s'} \cdot g_3^{s_2} \\ C_1 = g_1^{s_1 w_1} g_1^{s_1 w_2 rcv} \cdot g_2^{s' w_1} g_2^{s' w_2 rcv} \cdot g_3^{s_2 w_1} g_3^{s_2 w_4 \sigma} \\ C_2 = g_1^{s_1 w_3} \cdot g_2^{s' w_3} \cdot g_3^{s_2 w_3} \\ C_3 = e(g_1, h_1)^{\alpha s_1} \cdot m \end{cases}$, 其中, $s' \leftarrow_R \mathbb{Z}_N$.

注 9. 半功能 3 型的 dk_{ρ_v} 无法解密半功能 1 型的 ct, 即 $\mathrm{Game}_{2,D,3}$ 中敌手获得的 dk_{ρ_v} 不能解密 ct.

引理 1. $\mathrm{Game}_{\mathrm{real}}$ 过渡到 Game_1. 基于 SD 假设, 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{real}}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_1}(\lambda)\right| \leqslant \mathrm{Adv}_{\mathcal{B}_1}^{\mathrm{SD}}(\lambda).$$

证明: 假设有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{real}}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_1}(\lambda)\right| = \epsilon$, 而 ϵ 是一个不可忽略的值.

即存在一个 PPT 敌手 $\mathcal{B}_1$ 使得 $\mathrm{Adv}_{\mathcal{B}_1}^{\mathrm{SD}}(\lambda) = \epsilon$, 如下所示.

$\mathcal{B}_1$ 被给定 g_1, g_2, g_3 和 h_1, h_{12}, h_3, 取 $w_1, w_2, w_3, w_4, \alpha \leftarrow_R \mathbb{Z}_N$. $\mathcal{B}_1$ 发送 $\mathrm{mpk} = (g_1, g_1^{w_1}, g_1^{w_2}, g_1^{w_3}, g_1^{w_4}, e(g_1, h_1)^{\alpha})$ 给 $\mathcal{A}$, 并且秘密储存 $\mathrm{msk} = (h_1, h_3, g_3, w_1, w_2, w_3, w_4, h_1^{\alpha})$.

在 $\mathcal{A}$ 对 $\sigma_i, i \in [E]$ 进行 ek 问询后, $\mathcal{B}_1$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v, v \in [D]$ 进行 dk 问询后, $\mathcal{B}_1$ 像算法 RKGen 一样模拟出 dk_{ρ_v}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0, rcv_0, \sigma_0), (m_1, rcv_1, \sigma_1))$ 后, $\mathcal{B}_1$ 取 $\beta \leftarrow_R \{0,1\}$, 并模拟出 ct_{β}, 具体如下.

取 $s_2 \leftarrow_R \mathbb{Z}_N$, 然后用 SD 假设的挑战 T 生成 ct_{β}, 如下所示.

$$\begin{cases} C_0 = T \cdot g_3^{s_2} \\ C_1 = T^{w_1} T^{w_2 rcv_{\beta}} \cdot g_3^{s_2 w_1} g_3^{s_2 w_4 \sigma_{\beta}} \\ C_2 = T^{s_1 w_3} \cdot g_3^{s_2 w_3} \\ C_3 = e(T, h_1^{\alpha}) \cdot m_{\beta} \end{cases}.$$

$\mathcal{B}_1$ 将 ct_{β} 发回 $\mathcal{A}$.

观察到如果 $T = g_1^{s_1}$ (其中 $s_1 \leftarrow_R \mathbb{Z}_N$), 则 ct_{β} 与 $\mathrm{Game}_{\mathrm{real}}$ 相同; 如果 $T = g_1^{s_1} \cdot g_2^{s'}$ (其中 $s_1, s' \leftarrow_R \mathbb{Z}_N$), 则 ct_{β} 与 Game_1 相同. 因此成功构造了能攻破 SD 假设的敌手 $\mathcal{B}_1$, 这与困难假设相矛盾.

引理 2. $\mathrm{Game}_{2,j,0}$ 过渡到 $\mathrm{Game}_{2,j,1}$. 基于 SD 假设, 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j,0}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j,1}}(\lambda)\right| \leqslant \mathrm{Adv}_{\mathcal{B}_2}^{\mathrm{SD}}(\lambda).$$

证明: 假设有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j,0}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j,1}}(\lambda)\right| = \epsilon$, 而 ϵ 是一个不可忽略的值.

接下来构造一个 PPT 敌手 $\mathcal{B}_2$ 使得 $\mathrm{Adv}_{\mathcal{B}_2}^{\mathrm{SD}}(\lambda) = \epsilon$, 如下所示.

$\mathcal{B}_2$ 被给定 h_1, h_2, h_3 和 g_1, g_{12}, g_3, 取 $w_1, w_2, w_3, w_4, \alpha \leftarrow_R \mathbb{Z}_N$. $\mathcal{B}_2$ 发送 $\mathrm{mpk} = (g_1, g_1^{w_1}, g_1^{w_2}, g_1^{w_3}, g_1^{w_4}, e(g_1, h_1)^{\alpha})$ 给 $\mathcal{A}$, 并且秘密储存 $\mathrm{msk} = (h_1, h_3, g_3, w_1, w_2, w_3, w_4, h_1^{\alpha})$.

在 $\mathcal{A}$ 对 $\sigma_i, i \in [E]$ 进行 ek 问询后, $\mathcal{B}_2$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v, v \in [D]$ 进行 dk 问询后, $\mathcal{B}_2$ 对 $v \in [j-1]$ 模拟 dk_{ρ_v}, 取 $r_1, \alpha_v', r_2 \leftarrow_R \mathbb{Z}_N$, 然后生成 dk_{ρ_v}:

$$\begin{cases} K_0^1 = h_1^{r_1} \cdot h_3^{r_2} \\ K_1^1 = h_1^{r_1 w_1} h_1^{r_1 w_2 \rho_v} h_1^{\alpha} \cdot h_2^{\alpha_v'} \cdot h_3^{r_2 w_1} \\ K_2^1 = h_1^{r_1 w_3} \cdot h_3^{r_2 w_4} h_3^{r_2 w_3} \end{cases}.$$

$\mathcal{B}_2$ 对于 $v=j$ 模拟 dk_{ρ_v}, 取 $r_2 \leftarrow_R \mathbb{Z}_N$, 然后用 SD 假设的挑战 T 生成 dk_{ρ_v}, 如下所示.

$$\begin{cases} K_0^1 = T \cdot h_3^{r_2} \\ K_1^1 = T^{w_1} T^{w_2 \rho_v} h_1^{\alpha} \cdot h_3^{r_2 w_1} \\ K_2^1 = T^{w_3} \cdot h_3^{r_2 w_4} h_3^{r_2 w_3} \end{cases}.$$

$\mathcal{B}_2$ 对于 $v \in \{j+1, \ldots, D\}$ 像实际算法一样地模拟出 dk_{ρ_v}. 然后 $\mathcal{B}_2$ 将 $\mathrm{dk}_{\rho_v}, v \in [D]$ 发送回 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0, rcv_0, \sigma_0), (m_1, rcv_1, \sigma_1))$ 后, $\mathcal{B}_2$ 取 $\beta \leftarrow_R \{0,1\}$, 并模拟出 ct_β, 取 $s_{12}, s_2 \leftarrow_R \mathbb{Z}_N$, 然后生成 ct_β, 如下所示.

$$\begin{cases} C_0 = g_{12}^{s_{12}} \cdot g_3^{s_2} \\ C_1 = g_{12}^{s_{12} w_1} g_{12}^{s_{12} w_2 rcv_\beta} \cdot g_3^{s_2 w_1} g_3^{s_2 w_4 \sigma_\beta} \\ C_2 = g_{12}^{s_{12} w_3} \cdot g_3^{s_2 w_3} \\ C_3 = e(g_{12}^{s_{12}}, h_1^{\alpha}) \cdot m_\beta \end{cases}.$$

$\mathcal{B}_2$ 将 ct_β 发送回 $\mathcal{A}$.

观察到如果 $T = h_1^{r_1}$ (其中 $r_1 \leftarrow_R \mathbb{Z}_N$), dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.0}$ 相同; 如果 $T = h_1^{r_1} \cdot h_2^{r'}$ (其中 $r_1, r' \leftarrow_R \mathbb{Z}_N$), 那么 dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.1}$ 相同. 然后就可以成功地构造 $\mathcal{B}_2$ 来攻破 SD 假设, 而这违反了攻破 SD 假设很困难的事实.

引理 3. $\mathrm{Game}_{2,j.1}$ 过渡到 $\mathrm{Game}_{2,j.2}$. 基于 SD 假设, 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.1}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)\right| = 0.$$

证明:

由 $\mathrm{Game}_{2,j.1}$ 过渡到 $\mathrm{Game}_{2,j.2}$ 的过程中, 唯一的区别在于 dk_{ρ_j} 的分量 K_1^1 的分布.

在 $\mathrm{Game}_{2,j.1}$ 中 $K_1^1 = h_1^{r_1 w_1} h_1^{r_1 w_2 \rho_j} h_1^{\alpha} \cdot h_2^{r' w_1} h_2^{r' w_2 \rho_j} \cdot h_3^{r_2 w_1}$; 在 $\mathrm{Game}_{2,j.2}$ 中 $K_1^1 = h_1^{r_1 w_1} h_1^{r_1 w_2 \rho_j} h_1^{\alpha} \cdot h_2^{r' w_1} h_2^{r' w_2 \rho_j} h_2^{\alpha'_v} \cdot h_3^{r_2 w_1}$.

观察得到, 仅 H_{p_2} 的部分有改变. 根据中国剩余定理, 只需关注到 dk_{ρ_v} 和 ct 中 H_{p_2} 的部分.

对于 dk_{ρ_v} ($v \neq j$) 分别为正常型和半功能 3 型, 其中包含 H_{p_2} 的部分分别为:

$$v < j(\text{半功能3型}) : h_2^{\alpha'_v},$$

$$v > j(\text{正常型}) : h_2^0.$$

即, 只有 dk_{ρ_j} 和 ct 中包括 w_1 和 w_2 的信息. 根据 IB-ME 的不匹配条件以及 $\alpha\text{-}privacy(mod\, p_2)$[15], 可以得出 $h_2^{r' w_1} h_2^{r' w_2 \rho_j}$ 与 $h_2^{r' w_1} h_2^{r' w_2 \rho_j} h_2^{\alpha'_j}$ 分布完全相同, 因此 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.1}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)\right| = 0$.

引理 4. $\mathrm{Game}_{2,j.2}$ 过渡到 $\mathrm{Game}_{2,j.3}$. 基于 SD 假设, 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.3}}(\lambda)\right| \leqslant \mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda).$$

证明: 假设有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.3}}(\lambda)\right| = \epsilon$, 而 ϵ 是一个不可忽略的值.

接下来构造一个 PPT 敌手 $\mathcal{B}_3$ 使得 $\mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda) = \epsilon$, 如下所示.

$\mathcal{B}_3$ 被给定 h_1, h_2, h_3 和 g_1, g_{12}, g_3, 取 $w_1, w_2, w_3, w_4, \alpha \leftarrow_R \mathbb{Z}_N$. $\mathcal{B}_3$ 发送 $\mathrm{mpk}(g_1, g_1^{w_1}, g_1^{w_2}, g_1^{w_3} g_1^{w_4}, e(g_1, h_1)^{\alpha})$ 给 $\mathcal{A}$, 并且秘密储存 $\mathrm{msk} = (h_1, h_3, g_3, w_1, w_2, w_3, w_4, h_1^{\alpha})$.

在 $\mathcal{A}$ 对 $\sigma_i, i \in [E]$ 进行 ek 问询后, $\mathcal{B}_3$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v, v \in [D]$ 进行 dk 问询后, $\mathcal{B}_3$ 对 $v \in [j-1]$ 模拟 dk_{ρ_v}, 取 $r_1, \alpha'_v, r_2 \leftarrow_R \mathbb{Z}_N$, 然后生成 dk_{ρ_v}:

$$\begin{cases} K_0^1 = h_1^{r_1} \cdot h_3^{r_2} \\ K_1^1 = h_1^{r_1 w_1} h_1^{r_1 w_2 \rho_v} h_1^{\alpha} \cdot h_2^{\alpha'_v} \cdot h_3^{r_2 w_1} \\ K_2^1 = h_1^{r_1 w_3} \cdot h_3^{r_2 w_4} h_3^{r_2 w_3} \end{cases}.$$

$\mathcal{B}_3$ 对于 $v=j$ 模拟 dk_{ρ_v}, 取 $r_2 \leftarrow_R \mathbb{Z}_N$, 然后用 SD 假设的挑战 T 生成 dk_{ρ_v}, 如下所示:

$$\begin{cases} K_0^1 = T \cdot h_3^{r_2} \\ K_1^1 = T^{w_1} T^{w_2 \rho_v} h_1^{\alpha} \cdot h_2^{\alpha'_v} \cdot h_3^{r_2 w_1} \\ K_2^1 = T^{w_3} \cdot h_3^{r_2 w_4} h_3^{r_2 w_3} \end{cases}.$$

$\mathcal{B}_3$ 对于 $v \in \{j+1, \ldots, D\}$ 像实际算法一样模拟出 dk_{ρ_v}. 然后 $\mathcal{B}_3$ 将 $\mathrm{dk}_{\rho_v}, v \in [D]$ 发送回 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0, rcv_0, \sigma_0), (m_1, rcv_1, \sigma_1))$ 后, $\mathcal{B}_3$ 取 $\beta \leftarrow_R \{0,1\}$, 并模拟出 ct_β, 具体如下.

取 $s_{12}, s_2 \leftarrow_R \mathbb{Z}_N$, 然后生成 ct_β, 如下所示.

$$\begin{cases} C_0 = g_{12}^{s_{12}} \cdot g_3^{s_2} \\ C_1 = g_{12}^{s_{12}w_1} g_{12}^{s_{12}w_2 rcv_\beta} \cdot g_3^{s_2 w_1} g_3^{s_2 w_4 \sigma_\beta} \\ C_2 = g_{12}^{s_{12}w_3} \cdot g_3^{s_2 w_3} \\ C_3 = e(g_{12}^{s_{12}}, h_1^\alpha) \cdot m_\beta \end{cases}.$$

$\mathcal{B}_3$ 将 ct_β 发送回 $\mathcal{A}$.

观察到如果 $T = h_1^{r_1} \cdot h_2^{r'}$ $\left(\text{其中 } r_1, r' \leftarrow_R \mathbb{Z}_N\right)$, 那么 dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.2}$ 相同; 如果 $T = h_1^{r_1}$ (其中 $r_1 \leftarrow_R \mathbb{Z}_N$), dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.3}$ 相同. 然后就可以成功地构造 $\mathcal{B}_3$ 来攻破 SD 假设, 而这违反了攻破 SD 假设很困难的事实.

引理 5. $\mathrm{Game}_{2,D.3}$ 过渡到 $\mathrm{Game}_{\mathrm{final}}$. 有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{final}}}(\lambda) - \mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,D.3}}(\lambda)\right| = 0$.

即, $\mathrm{Game}_{\mathrm{final}}$ 和 $\mathrm{Game}_{2,D.3}$ 分布完全相同.

证明: 由观察易得 $ct = (C_0, C_1, C_2, C_3)$ 在 $\mathrm{Game}_{\mathrm{final}}$ 和 $\mathrm{Game}_{2,D.3}$ 中分布完全相同.

定理 1. 基于 SD 假设, 方案 Π_{C1} 满足隐私性.

证明: 根据引理 1–引理 5 可得, 对于任何 PPT 敌手 $\mathcal{A}$, 都有:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{priv}}}(\lambda) = \left|\Pr\left[\mathrm{Game}_{\mathcal{A}}^{\mathrm{priv}}(\lambda) = 1\right] - \frac{1}{2}\right| \leqslant \mathrm{Adv}_{\mathcal{B}_1}^{\mathrm{SD}}(\lambda) + D \cdot \mathrm{Adv}_{\mathcal{B}_2}^{\mathrm{SD}}(\lambda) + D \cdot \mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda) \leqslant negl(\lambda).$$

根据隐私性定义 (定义 5), 方案 Π_{C1} 基于 SD 假设满足隐私性.

4.2.2 真实性证明

定理 2. 对于任何 PPT 敌手 $\mathcal{A}$, 有 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{auth}}}(\lambda) = \Pr\left[\mathrm{Game}_{\mathcal{A}}^{\mathrm{auth}}(\lambda) = 1\right] \leqslant \mathrm{Adv}_{\mathcal{B}}^{\mathrm{IBE}_{C1}}(\lambda)$.

其中 $\mathcal{B}$ 在下述的证明中定义.

证明: 真实性可以规约到基于 SD 假设的 σ-*snd* 对所对应的 IBE 方案的安全性, 它被嵌入到 IB-ME 方案 Π_{C1} 中.

假设 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{auth}}}(\lambda) = \epsilon$, 而 ϵ 是一个不可忽略的值.

则构造一个敌手 $\mathcal{B}$ 使得 $\mathrm{Adv}_{\mathcal{B}}^{\mathrm{IBE}}(\lambda) = \epsilon$, 具体如下.

在 $\mathcal{A}$ 问询 $(\mathrm{ct}_{rcv,\sigma}, \rho, snd)$ 后, $\mathcal{B}$ 跟真实的算法一样生成 dk_ρ, 并将 dk_ρ 发回给 $\mathcal{A}$. 然后 $\mathcal{A}$ 有的 ϵ 可能性发现 $\sigma^* \neq snd$, 这样 σ^* 在用 *snd* 解密时对生成 $\mathrm{ct}_{rcv,\sigma}$ 也有效, 然后 $\mathcal{A}$ 把 σ^* 发送给 $\mathcal{B}$. 需要注意 σ 和 σ^* 都对于 $\mathrm{ct}_{rcv,\sigma}$ 是有效的意味着对于一个在基础 IBE 中与 *snd* 相关的密文而言, 有两个有效的密钥分别与 σ 和 σ^* 相关. 因此, $\mathcal{B}$ 可以对 σ^* 进行密钥问询, 并且挑战 (m_0, σ') 和 (m_1, σ). 然后 $\mathcal{B}$ 可以通过与 σ^* 相关的密钥来轻易地区分挑战密文. 因此产生矛盾.

4.3 参数更短的方案: 构造 Π_{C2}

本节将介绍非对称合数阶群上的方案 Π_{C2} 的构造. 方案 Π_{C2} 主要通过减少参数大小来改进效率. 具体的改进见表 2.

表 2 方案 Π_{C1} 与 Π_{C2} 的参数大小比较

参数大小	$\lvert\mathrm{ek}_\sigma\rvert$	$\lvert\mathrm{dk}_\rho\rvert$	$\lvert\mathrm{ct}\rvert$
Π_{C1}	$4\lvert G\rvert$	$9\lvert H\rvert$	$8\lvert G\rvert + 1\lvert G_T\rvert$
Π_{C2}	$3\lvert G\rvert$	$8\lvert H\rvert$	$6\lvert G\rvert + 1\lvert G_T\rvert$

以下是 Π_{C2} 的算法.

- 初始化 $\mathrm{Setup}(\lambda)$: 运行群生成元 $\mathbb{G} = (N = p_1 p_2 p_3, G, H, G_T, e, g, h) \leftarrow \mathcal{G}(\lambda)$, 然后输出 $\mathrm{pp} = \mathbb{G}$.

取 $w_1, w_2, w_3, w_4, \alpha \leftarrow {}_R\mathbb{Z}_N$, 输出 $\mathrm{mpk} = (g_1, g_1^{w_1}, g_1^{w_2}, g_1^{w_3}, g_1^{w_4}, e(g_1, h_1)^\alpha)$, 储存 $\mathrm{msk} = (h_1, h_3, g_3, w_1, w_2, w_3, w_4, h_1^\alpha)$.

- 生成加密密钥 $\mathrm{SKGen}(\mathrm{pp}, \mathrm{msk}, \sigma)$: 取 $s_2 \leftarrow_R \mathbb{Z}_N$, 然后输出:

$$\mathrm{ek}_\sigma=\left(K_0^2=g_3^{s_2w_3}g_3^{s_2w_4\sigma},\ K_1^2=g_3^{s_2}\right).$$

● 生成解密密钥 $\mathrm{RKGen}(\mathrm{pp},\mathrm{msk},\rho)$: 取 $t,r_1,r_2\leftarrow_R\mathbb{Z}_N$, 然后输出:

$$\mathrm{dk}_\rho=(K_0^1=h_1^{r_1}\cdot h_3^{r_2w_3},K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_3^{r_2},K_2^1=h_1^{r_1t}\cdot h_3^{r_2w_4}).$$

● 加密 $\mathrm{Enc}(\mathrm{pp},\mathrm{mpk},\mathrm{ek}_\sigma,rcv,m)$: 取 $s_1\leftarrow{}_R\mathbb{Z}_N$, 然后输出:

$$\mathrm{ct}=(C_0=g_1^{s_1}\cdot K_0^2,C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv},C_2=K_1^2,C_3=e(g_1,h_1^{\alpha})^{s_1}\cdot m).$$

● 解密 $\mathrm{Dec}(\mathrm{pp},\mathrm{dk}_\rho,snd,\mathrm{ct})$: 计算 $m=C_3/(e(C_0,K_1^1)/e(C_1,K_0^1)\cdot e(C_2,K_0^1)\cdot e(C_2,(K_2^1)^{snd}))$.

正确性如下所示.

$$\begin{aligned}&e(C_0,K_1^1)/e(C_1,K_0^1)\cdot e(C_2,K_0^1)\cdot e(C_2,(K_2^1)^{snd})\\&=e(g_1^{(s_1)}\cdot g_3^{(s_2w_3)}\cdot g_3^{(s_2w_4\sigma)},h_1^{(r_1w_1)}\cdot h_1^{(r_1w_2\rho)}\cdot h_1^{\alpha}\cdot h_3^{(r_2)})\\&\quad/e(g_1^{(s_1w_1)}\cdot g_1^{(s_1w_2\cdot rcv)},h_1^{(r_1)}\cdot h_3^{(r_2w_3)})\cdot e(g_3^{(s_2)},h_1^{(r_1)}\cdot h_3^{(r_2w_3)})\\&\quad\cdot e(g_3^{(s_2)},h_1^{(r_1\cdot t\cdot snd)}\cdot h_3^{(r_2w_4\cdot snd)})\\&=e(g_1,h_1)^{\alpha s_1}.\end{aligned}$$

4.4 安全性分析

与上文中方案 Π_{C1} 的安全性分析相似, 将分别分析方案 Π_{C2} 满足隐私性和安全性.

4.4.1 隐私性证明

为了证明隐私性, 此处仍采取双系统加密方法, 借助的游戏序列与第 4.2.1 节中的相同, 此处省略.

隐私性证明中 D 为 dk 问询次数的上限; 涉及的 $\mathrm{ek}_\sigma,\mathrm{dk}_\rho$ 和 ct 的形式如下.

● ek_σ 的形式:

$$\begin{cases}K_0^2=g_3^{s_2w_3}g_3^{s_2w_4\sigma}\\K_1^2=g_3^{s_2}\end{cases}.$$

● dk_ρ 的 4 种形式:

① 正常型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_3^{r_2w_3}\\K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_3^{r_2}\\K_2^1=h_1^{r_1t}\cdot h_3^{r_2w_4}\end{cases}$.

② 半功能 1 型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_2^{r'}\cdot h_3^{r_2w_3}\\K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho}\cdot h_3^{r_2}\\K_2^1=h_1^{r_1t}\cdot h_2^{r't}\cdot h_3^{r_2w_4}\end{cases}$, 其中, $r'\leftarrow{}_R\mathbb{Z}_N$.

③ 半功能 2 型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_2^{r'}\cdot h_3^{r_2w_3}\\K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho}h_2^{\alpha'}\cdot h_3^{r_2}\\K_2^1=h_1^{r_1t}\cdot h_2^{r't}\cdot h_3^{r_2w_4}\end{cases}$, 其中, $r',\alpha'\leftarrow_R\mathbb{Z}_N$.

④ 半功能 3 型 $\begin{cases}K_0^1=h_1^{r_1}\cdot h_3^{r_2w_3}\\K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho}h_1^{\alpha}\cdot h_2^{\alpha'}\cdot h_3^{r_2}\\K_2^1=h_1^{r_1t}\cdot h_3^{r_2w_4}\end{cases}$, 其中, $\alpha'\leftarrow_R\mathbb{Z}_N$.

● ct 的 2 种形式:

① 正常型 $\begin{cases}C_0=g_1^{s_1}\cdot g_3^{s_2w_3}g_3^{s_2w_4\sigma}\\C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv}\\C_2=g_3^{s_2}\\C_3=e(g_1,h_1^{\alpha})^{s_1}\cdot m\end{cases}$.

② 半功能 1 型 $\begin{cases}C_0=g_1^{s_1}\cdot g_2^{s'}\cdot g_3^{s_2w_3}g_3^{s_2w_4\sigma}\\C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv}\cdot g_2^{s'w_1}g_2^{s'w_2rcv}\\C_2=g_3^{s_2}\\C_3=e(g_1,h_1^{\alpha})^{s_1}\cdot m\end{cases}$, 其中, $s'\leftarrow_R\mathbb{Z}_N$.

引理 6. $\text{Game}_{\text{real}}$ 过渡到 Game_1. 基于 SD 假设, 有:

$$\left|\text{Adv}_{\mathcal{A}}^{\text{Game}_1}(\lambda)-\text{Adv}_{\mathcal{A}}^{\text{Game}_{\text{real}}}(\lambda)\right|\leqslant \text{Adv}_{\mathcal{B}_1}^{\text{SD}}(\lambda).$$

证明: 假设有 $\left|\text{Adv}_{\mathcal{A}}^{\text{Game}_1}(\lambda)-\text{Adv}_{\mathcal{A}}^{\text{Game}_{\text{real}}}(\lambda)\right|=\epsilon$, 而 ϵ 是一个不可忽略的值.

即存在 PPT 敌手 $\mathcal{B}_1$ 使得 $\text{Adv}_{\mathcal{B}_1}^{\text{SD}}(\lambda)=\epsilon$, 具体如下.

$\mathcal{B}_1$ 被给定 g_1,g_2,g_3 和 h_1,h_{12},h_3, 然后取 $w_1,w_2,w_3,w_4,\alpha\leftarrow_R\mathbb{Z}_N$. 将 $\text{mpk}=(g_1,g_1^{w_1},g_1^{w_2},g_1^{w_3},g_1^{w_4},e(g_1,h_1)^{\alpha})$ $\mathcal{B}_1$ 发送给 $\mathcal{A}$, 并秘密储存 $\text{msk}=(h_1,h_3,g_3,w_1,w_2,w_3,w_4,h_1^{\alpha})$.

在 $\mathcal{A}$ 对 $\sigma_i,i\in[E]$ 进行 ek 问询后, $\mathcal{B}_1$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v,v\in[D]$ 进行 dk 问询后, $\mathcal{B}_1$ 像算法 RKGen 一样模拟出 dk_{ρ_v}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0,rcv_0,\sigma_0),(m_1,rcv_1,\sigma_1))$ 后, $\mathcal{B}_1$ 取 $\beta\leftarrow_R\{0,1\}$, 并模拟出 ct_{β}, 具体如下.

取 $s_2\leftarrow_R\mathbb{Z}_N$, 然后用 SD 假设的挑战 T 生成 ct_{β}, $\mathcal{B}_1$ 将 ct_{β} 发回 $\mathcal{A}$. ct_{β} 如下所示.

$$\begin{cases}C_0=T\cdot g_3^{s_2w_3}g_3^{s_2w_4\sigma_{\beta}}\\ C_1=T^{w_1}T^{w_2rcv_{\beta}}\\ C_2=g_3^{s_2}\\ C_3=e(T,h_1^{\alpha})\cdot m\end{cases}.$$

观察到如果 $T=g_1^{s_1}$ (其中 $s_1\leftarrow_R\mathbb{Z}_N$) 则 ct_{β} 与 $\text{Game}_{\text{real}}$ 相同; 如果 $T=g_1^{s_1}\cdot g_2^{s'}$ (其中 $s_1,s'\leftarrow_R\mathbb{Z}_N$), 则 ct_{β} 与 Game_1 相同. 接下来就可以成功地建立一个敌手 $\mathcal{B}_1$ 来攻破 SD 假设, 而这违反了攻破 SD 假设很困难的事实.

引理 7. $\text{Game}_{2,j.0}$ 过渡到 $\text{Game}_{2,j.1}$. 基于 SD 假设, 有 $\left|\text{Adv}_{\mathcal{A}}^{\text{Game}_{2,j.0}}(\lambda)-\text{Adv}_{\mathcal{A}}^{\text{Game}_{2,j.1}}(\lambda)\right|\leqslant\text{Adv}_{\mathcal{B}_2}^{\text{SD}}(\lambda)$.

证明: 假设有 $\left|\text{Adv}_{\mathcal{A}}^{\text{Game}_{2,j}}(\lambda)-\text{Adv}_{\mathcal{A}}^{\text{Game}_{2,j-1}}(\lambda)\right|=\epsilon$, 而 ϵ 是一个不可忽略的值.

接下来构造一个 PPT 敌手 $\mathcal{B}_2$ 使得 $\text{Adv}_{\mathcal{B}_2}^{\text{SD}}(\lambda)=\epsilon$, 如下所示.

$\mathcal{B}_2$ 被给定 h_1,h_2,h_3 和 g_1,g_{12},g_3, 取 $w_1,w_2,w_3,w_4,\alpha,\alpha_2\leftarrow_R\mathbb{Z}_N$.$\mathcal{B}_2$ 发送 $\text{mpk}=(g_1,g_1^{w_1},g_1^{w_2},g_1^{w_3},g_1^{w_4},e(g_1,h_1)^{\alpha})$给 $\mathcal{A}$, 并且秘密储存 $\text{msk}=(h_1,h_3,g_3,w_1,w_2,w_3,w_4,h_1^{\alpha},g_3^{\alpha_2})$.

在 $\mathcal{A}$ 对 $\sigma_i,i\in[E]$ 进行 ek 问询后, $\mathcal{B}_2$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v,v\in[D]$ 进行 dk 问询后, $\mathcal{B}_2$ 对 $v\in[j-1]$ 模拟 dk_{ρ_v}, 如下所示.

取 $t,r_1,r_2,\alpha_v'\leftarrow_R\mathbb{Z}_N$, 然后生成 dk_{ρ_v}:

$$\begin{cases}K_0^1=h_1^{r_1}\cdot h_3^{r_2w_3}\\ K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho_v}h_1^{\alpha}\cdot h_2^{\alpha_v'}\cdot h_3^{r_2}\\ K_2^1=h_1^{r_1t}\cdot h_3^{r_2w_4}\end{cases}.$$

$\mathcal{B}_2$ 对于 $v=j$ 模拟 dk_{ρ_v}: 取 $r_2\leftarrow_R\mathbb{Z}_N$, 然后用 SD 假设的挑战 T 生成 dk_{ρ_v}, 如下所示.

$$\begin{cases}K_0^1=T\cdot h_3^{r_2w_3}\\ K_1^1=T^{w_1}T^{w_2\rho_v}h_1^{\alpha}\cdot h_3^{r_2}\\ K_2^1=T^{t}\cdot h_3^{r_2w_2}\end{cases}.$$

$\mathcal{B}_2$ 对于 $v\in\{j+1,\ldots,D\}$ 像实际算法一样地模拟出 dk_{ρ_v}. 然后 $\mathcal{B}_2$ 将 $\text{dk}_{\rho_v},v\in[D]$ 发送回 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0,rcv_0,\sigma_0),(m_1,rcv_1,\sigma_1))$ 后, $\mathcal{B}_2$ 取 $\beta\leftarrow_R\{0,1\}$, 并模拟出 ct_{β}, 具体如下.

取 $s_{12},s_2\leftarrow_R\mathbb{Z}_N$, 然后生成 ct_{β}, $\mathcal{B}_2$ 将 ct_{β} 发送回 $\mathcal{A}$. ct_{β} 如下所示.

$$\begin{cases}C_0=g_1^{s_1}\cdot g_2^{s'}\cdot g_3^{s_2w_3}g_3^{s_2w_4\sigma_{\beta}}\\ C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv_{\beta}}\cdot g_2^{s'w_1}g_2^{s'w_2rcv_{\beta}}\\ C_2=g_3^{s_2}\\ C_3=e(g_1,h_1^{\alpha})^{s_1}\cdot m_{\beta}\end{cases}.$$

观察到如果 $T=h_1^{r_1}$ (其中 $r_1\leftarrow_R\mathbb{Z}_N$), dk_{ρ_v} 跟 $\text{Game}_{2,j.0}$ 相同; 如果 $T=h_1^{r_1}\cdot h_2^{r'}$ (其中 $r_1,r'\leftarrow_R\mathbb{Z}_N$), 那么 dk_{ρ_v} 跟 $\text{Game}_{2,j.1}$ 相同. 然后就可以成功地构造 $\mathcal{B}_2$ 来攻破 SD 假设, 而这违反了攻破 SD 假设很困难的事实.

引理 8. $\text{Game}_{2,j.1}$ 过渡到 $\text{Game}_{2,j.2}$. 基于 SD 假设, 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.1}}(\lambda)-\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)\right|=0.$$

证明:

由 $\mathrm{Game}_{2,j.1}$ 过渡到 $\mathrm{Game}_{2,j.2}$ 的过程中, 唯一的区别在于 dk_{ρ_j} 的分量 K_1^1 的分布:

在 $\mathrm{Game}_{2,j.1}$ 中 $K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho_j}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho_j}\cdot h_3^{r_2}$; 在 $\mathrm{Game}_{2,j.2}$ 中 $K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho_j}h_1^{\alpha}\cdot h_2^{r'w_1}h_2^{r'w_2\rho_j}h_2^{\alpha'_v}\cdot h_3^{r_2}$.

观察得到, 仅 H_{p_2} 的部分有改变. 根据中国剩余定理, 只需关注到 dk_{ρ_v} 和 ct 中 H_{p_2} 的部分.

对于 dk_{ρ_v} ($v\neq j$) 分别为正常型和半功能 3 型, 其中包含 H_{p_2} 的部分分别为:

$$v<j\,(\text{半功能 3 型}):\ h_2^{\alpha'_v},$$

$$v>j\,(\text{正常型}):\ h_2^{0}.$$

即, 只有 dk_{ρ_j} 和 ct 中包括 w_1 和 w_2 的信息. 根据 IB-ME 的不匹配条件以及 α-*privacy* $(\mathrm{mod}\ p_2)$[15], 可以得出 $h_2^{r'w_1}h_2^{r'w_2\rho_j}$ 与 $h_2^{r'w_1}h_2^{r'w_2\rho_j}h_2^{\alpha'}$ 分布完全相同, 因此 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.1}}(\lambda)-\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)\right|=0$.

引理 9. $\mathrm{Game}_{2,j.2}$ 过渡到 $\mathrm{Game}_{2,j.3}$. 基于 SD 假设, 有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)-\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.3}}(\lambda)\right|\leqslant\mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda)$.

证明: 假设有 $\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.2}}(\lambda)-\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,j.3}}(\lambda)\right|=\epsilon$, 而 ϵ 是一个不可忽略的值.

接下来构造一个 PPT 敌手 $\mathcal{B}_3$ 使得 $\mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda)=\epsilon$, 如下所示.

$\mathcal{B}_3$ 被给定 h_1,h_2,h_3 和 g_1,g_{12},g_3 , 取 $w_1,w_2,w_3,w_4,\alpha\leftarrow_R\mathbb{Z}_N$.$\mathcal{B}_3$ 发送 $\mathrm{mpk}(g_1,g_1^{w_1},g_1^{w_2},g_1^{w_3},g_1^{w_4},e(g_1,h_1)^{\alpha})$ 给 $\mathcal{A}$, 并且秘密储存 $\mathrm{msk}=(h_1,h_3,g_3,w_1,w_2,w_3,w_4,h_1^{\alpha})$.

在 $\mathcal{A}$ 对 $\sigma_i,i\in[E]$ 进行 ek 问询后, $\mathcal{B}_3$ 像算法 SKGen 一样模拟出 ek_{σ_i}, 并且将输出返回给 $\mathcal{A}$.

在 $\mathcal{A}$ 对 $\rho_v,v\in[D]$ 进行 dk 问询后, $\mathcal{B}_3$ 对 $v\in[j-1]$ 模拟 dk_{ρ_v}, 如下所示.

取 $t,r_1,r_2,\alpha'_v\leftarrow_R\mathbb{Z}_N$, 然后生成 dk_{ρ_v}:

$$\begin{cases}K_0^1=h_1^{r_1}\cdot h_3^{r_2w_3}\\ K_1^1=h_1^{r_1w_1}h_1^{r_1w_2\rho_v}h_1^{\alpha}\cdot h_2^{\alpha'_v}\cdot h_3^{r_2}\\ K_2^1=h_1^{r_1t}\cdot h_3^{r_2w_4}\end{cases}.$$

$\mathcal{B}_3$ 对于 $v=j$ 模拟 dk_{ρ_v}, 即, 用 SD 假设的挑战 T 生成 dk_{ρ_v}, 如下所示:

$$\begin{cases}K_0^1=T\cdot h_3^{r_2w_3}\\ K_1^1=T^{w_1+w_2\rho_v}h_1^{\alpha}\cdot h_2^{\alpha'_v}\cdot h_3^{r_2}\\ K_2^1=T^{t}\cdot h_3^{r_2w_4}\end{cases}.$$

$\mathcal{B}_3$ 对于 $v\in\{j+1,\ldots,D\}$ 像实际算法一样地模拟出 dk_{ρ_v}. 然后 $\mathcal{B}_3$ 将 $\mathrm{dk}_{\rho_v},v\in[D]$ 发送回 $\mathcal{A}$.

在 $\mathcal{A}$ 挑战 $((m_0,rcv_0,\sigma_0),(m_1,rcv_1,\sigma_1))$ 后, $\mathcal{B}_3$ 取 $\beta\leftarrow_R\{0,1\}$, 并模拟出 ct_{β}, 具体如下.

取 $s_{12},s_2\leftarrow_R\mathbb{Z}_N$, 然后生成 ct_{β}, 将 ct_{β} 发送回 $\mathcal{A}$. ct_{β} 如下所示.

$$\begin{cases}C_0=g_1^{s_1}\cdot g_2^{s'}\cdot g_3^{s_2w_3}g_3^{s_2w_4\sigma_{\beta}}\\ C_1=g_1^{s_1w_1}g_1^{s_1w_2rcv_{\beta}}\cdot g_2^{s'w_1}g_2^{s'w_2rcv_{\beta}}\\ C_2=g_3^{s_2}\\ C_3=e(g_1,h_1^{\alpha})^{s_1}\cdot m_{\beta}\end{cases}.$$

观察到如果 $T=h_1^{r_1}\cdot h_2^{r'}$ (其中 $r_1,r'\leftarrow_R\mathbb{Z}_N$), 那么 dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.2}$ 相同; 如果 $T=h_1^{r_1}$ (其中 $r_1\leftarrow_R\mathbb{Z}_N$), dk_{ρ_v} 跟 $\mathrm{Game}_{2,j.3}$ 相同. 然后就可以成功地构造 $\mathcal{B}_3$ 来攻破 SD 假设, 而这违反了攻破 SD 假设很困难的事实.

引理 10. $\mathrm{Game}_{2,j.D}$ 过渡到 $\mathrm{Game}_{\mathrm{final}}$. 有:

$$\left|\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{final}}}(\lambda)-\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game}_{2,D.3}}(\lambda)\right|=0,$$

即, $\mathrm{Game}_{\mathrm{final}}$ 和 $\mathrm{Game}_{2,D.3}$ 分布完全相同.

证明: 由观察易得 $\mathrm{ct}=(C_0,C_1,C_2,C_3)$ 在 $\mathrm{Game}_{\mathrm{final}}$ 和 $\mathrm{Game}_{2,D.3}$ 中分布完全相同.

定理 3. 基于 SD 假设, 方案 Π_{C2} 满足隐私性.

证明: 根据引理 6–引理 10 可得, 对于任何 PPT 敌手 $\mathcal{A}$, 都有:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game_{priv}}}(\lambda)=\left|\Pr\left[\mathrm{Game}_{\mathcal{A}}^{\mathrm{priv}}(\lambda)=1\right]-\frac{1}{2}\right|\leqslant \mathrm{Adv}_{\mathcal{B}_1}^{\mathrm{SD}}(\lambda)+\mathrm{D}\cdot\mathrm{Adv}_{\mathcal{B}_2}^{\mathrm{SD}}(\lambda)+\mathrm{D}\cdot\mathrm{Adv}_{\mathcal{B}_3}^{\mathrm{SD}}(\lambda)\leqslant negl(\lambda).$$

根据隐私性定义 (定义 5), 方案 Π_{C1} 基于 SD 假设满足隐私性.

4.4.2 真实性证明

定理 4. 对于任何 PPT 敌手 $\mathcal{A}$, 有:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game_{auth}}}(\lambda)=\Pr\left[\mathrm{Game}_{\mathcal{A}}^{\mathrm{auth}}(\lambda)=1\right]\leqslant \mathrm{Adv}_{\mathcal{B}}^{\mathrm{IBE}_{C2}}(\lambda),$$

其中, $\mathcal{B}$ 是针对第 2 层 IBE 方案的 PPT 敌手.

证明: 真实性可以规约到基于 SD 假设的 σ-snd 对所对应的 IBE 方案的安全性, 它被嵌入到这里的 IB-ME 方案中. 具体的证明几乎与定理 2 一样, 所以此处予以省略.

5 基于素数阶群的 IB-ME

本节基于上文合数阶群的方案在素数阶群上构造 IB-ME 方案, 构造过程中使用了 DPVS 技术. 这项技术通过将合数阶群版本中每一个的群元素替代成素数阶群版本中 4 个群元素, 将合数阶群方案模拟到素数阶群上.

除此之外, 由于观察到 IB-ME 的隐私性只需要考虑 *rcv*-ρ 对, 因为 σ-*snd* 对不需要向可信中心问询并且 IB-ME 中的密文可以通过 *rcv*-ρ 对隐藏 σ. 所以安全分析只需要一维对偶基. 这意味着只需要 3 个群元素就可以模拟合数阶版本中的一个群元素. 另外, 可以观察到对于第 2 层的 IBE 中 g_T^{α} 实际上是不必须的, 因为第 2 层的作用是签名, 而对于签名, g_T^{α} 可以设为 $g_T^0=[1]_T$. 因此, mpk 和 dk 中可以分别减少 1 个群元素.

通过上述处理, 使得本节素数阶群的 IB-ME 方案效率相较于现有方案[4]有显著提高.

5.1 构造 Π_{P1}

本节通过 DPVS 模拟第 4.3 节的方案 Π_{C2}, 提出了一个非对称素数阶群的 IB-ME 方案. 具体地说, 进行以下替换: $g_i\rightarrow g^{\mathbf{d}_i}, h_i\rightarrow h^{\mathbf{d}_i^*}$.

方案 Π_{P1} 由以下 5 个算法组成.

● 初始化 $\mathrm{Setup}(\lambda)$: 运行群生成元 $\mathbb{G}=(p,G,H,G_T,e,g,h)\leftarrow\mathcal{G}(\lambda)$, 然后输出 $\mathrm{pp}=\mathbb{G}$.

随机抽取对偶正交基 $(\mathbb{D},\mathbb{D}^*)\leftarrow_R\mathrm{Dual}\left(\mathbb{Z}_p^3\right)$. 用 $\mathbf{d}_1,\mathbf{d}_2,\mathbf{d}_3$ 表示 $\mathbb{D}$ 的元素并用 $\mathbf{d}_1^*,\mathbf{d}_2^*,\mathbf{d}_3^*$ 表示 $\mathbb{D}^*$ 的元素. 令 $g_T=e(g,h)^{\mathbf{d}_i,\mathbf{d}_i^*}$. 取 $w_1,w_2,w_3,w_4,\alpha\leftarrow_R\mathbb{Z}_p$, 然后输出 $\mathrm{mpk}=(g^{\mathbf{d}_1},g^{w_1\mathbf{d}_1},g^{w_2\mathbf{d}_1},g^{w_3\mathbf{d}_1},g^{w_4\mathbf{d}_1},e(g^{\mathbf{d}_1},h^{\mathbf{d}_1^*})^{\alpha})$ 储存 $\mathrm{msk}=(h^{\mathbf{d}_1^*},h^{\mathbf{d}_3^*},g^{\mathbf{d}_3},w_1,w_2,w_3,w_4,\alpha)$.

● 生成加密密钥 $\mathrm{SKGen}(\mathrm{pp},\mathrm{msk},\sigma)$: 取 $s_2\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{ek}_{\sigma}=(K_0^2=g^{s_2w_3\mathbf{d}_3}g^{s_2w_4\sigma\mathbf{d}_3},K_1^2=g^{s_2\mathbf{d}_3}).$$

● 生成解密密钥 $\mathrm{RKGen}(\mathrm{pp},\mathrm{msk},\rho)$: 取 $t,r_1,r_2\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{dk}_{\rho}=(K_0^1=h^{r_1\mathbf{d}_1^*}\cdot h^{r_2w_3\mathbf{d}_3^*},K_1^1=h^{r_1w_1\mathbf{d}_1^*}h^{r_1w_2\rho\mathbf{d}_1^*}h^{\alpha\mathbf{d}_1^*}\cdot h^{r_2\mathbf{d}_3^*},K_2^1=h^{r_1t\cdot\mathbf{d}_1^*}\cdot h^{r_2w_4\mathbf{d}_3^*}).$$

● 加密 $\mathrm{Enc}\left(\mathrm{pp},\mathrm{mpk}^{\mathrm{ek}}\mathrm{ek}_{\sigma},rcv,m\right)$: 取 $s_1\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{ct}=(C_0=g^{s_1\mathbf{d}_1}\cdot K_0^2,C_1=g^{s_1w_1\mathbf{d}_1}g^{s_1w_2rcv\mathbf{d}_1}C_2=K_1^2,C_3=e(g^{\mathbf{d}_1},h^{\alpha\mathbf{d}_1^*})^{s_1}\cdot m).$$

● 解密 $\mathrm{Dec}(\mathrm{pp},\mathrm{dk}_{\rho},snd,\mathrm{ct})$: 计算 $m=C_3/(e(C_0,K_1^1)/e(C_1,K_0^1)\cdot e(C_2,K_0^1)\cdot e(C_2,(K_2^1)^{snd}))$.

正确性:

$$\begin{aligned}&e(C_0,K_1^1)/e(C_1,K_0^1)\cdot e(C_2,K_0^1)\cdot e(C_2,(K_2^1)^{snd})\\&=e(g^{(s_1\mathbf{d}_1+(s_2w_3+s_2w_4\sigma)\mathbf{d}_3)},h^{((r_1w_1+r_1w_2\rho+\alpha)\mathbf{d}_1^*+r_2\mathbf{d}_3^*)})/e(g^{((s_1w_1+s_1w_2rcv)\mathbf{d}_1)},h^{(r_1\mathbf{d}_1^*+r_2w_3\mathbf{d}_3^*)})\\&\quad\cdot e(g^{(s_2\mathbf{d}_3)},h^{(r_1\mathbf{d}_1^*+r_2w_3\mathbf{d}_3^*)})\cdot e(g^{(s_2\mathbf{d}_3)},h^{(r_1t\cdot snd\cdot\mathbf{d}_1^*+r_2w_4snd\cdot\mathbf{d}_3^*)})\\&=g_T^{\alpha s_1}.\end{aligned}$$

5.2 安全性分析

定理 5. 基于 DS 假设, IB-ME 方案 Π_{P1} 满足隐私性和真实性.

证明: 隐私性的证明与合数阶版本对应, 在此予以省略. 以下是真实性证明.

定理 6. 对于任何 PPT 敌手 $\mathcal{A}$, 有:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Game_{auth}}}(\lambda)=\Pr\left[\mathrm{Game}_{\mathcal{A}}^{\mathrm{auth}}(\lambda)=1\right]\leqslant \mathrm{Adv}_{\mathcal{B}}^{\mathrm{IBE}_{P1}}(\lambda).$$

其中, $\mathcal{B}$ 是针对第 2 层 IBE 方案的 PPT 敌手.

证明: 真实性可以规约到基于 DS 假设 (或者说 SXDH 假设) 的 σ-*snd* 对所对应的素数阶群上的 IBE 方案的安全性, 它被嵌入到把本文素数阶群上的 IB-ME 方案中. 具体证明与定理 2 几乎相同, 此处予以省略.

5.3 构造 Π_{P2}

本节中提出了方案 Π_{C1} 的一个素数阶群上的版本

- 初始化 $\mathrm{Setup}(\lambda)$: 运行群生成元 $\mathbb{G}=(p,G,H,G_T,e,g,h)\leftarrow\mathcal{G}(\lambda)$, 然后输出 $\mathrm{pp}=\mathbb{G}$. 随机抽取对偶正交基 $(\mathbb{D},\mathbb{D}^*)\leftarrow_R\mathrm{Dual}\left(\mathbb{Z}_p^3\right)$. 用 $\mathbf{d}_1,\mathbf{d}_2,\mathbf{d}_3$ 表示 $\mathbb{D}$ 的元素并用 $\mathbf{d}_1^*,\mathbf{d}_2^*,\mathbf{d}_3^*$ 表示 $\mathbb{D}^*$ 的元素. 令 $g_T=e(g,h)^{\mathbf{d}_i,\mathbf{d}_i^*}$. 取 $w_1,w_2,w_3,w_4,\alpha\leftarrow_R\mathbb{Z}_p$, 然后输出 $\mathrm{mpk}=(g^{\mathbf{d}_1},g^{w_1\mathbf{d}_1},g^{w_2\mathbf{d}_1},g^{w_3\mathbf{d}_1},g^{w_4\mathbf{d}_1},e(g^{\mathbf{d}_1},h^{\mathbf{d}_1^*})^{\alpha})$, 储存 $\mathrm{msk}=\left(h^{\mathbf{d}_1^*},h^{\mathbf{d}_3^*},g^{\mathbf{d}_3},w_1,w_2,w_3,w_4,\alpha\right)$.
- 生成加密密钥 $\mathrm{SKGen}(\mathrm{pp},\ \mathrm{msk},\ \sigma)$: 取 $s_2\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{ek}_{\sigma}=(K_0^2=g^{s_2\mathbf{d}_3},K_1^2=g^{s_2w_1\mathbf{d}_3}g^{s_2w_4\sigma\mathbf{d}_3},K_2^2=g^{s_2w_3\mathbf{d}_3}).$$

- 生成解密密钥 $\mathrm{RKGen}(\mathrm{pp},\ \mathrm{msk},\ \rho)$: 取 $r_1,r_2\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{dk}_{\rho}=(K_0^1=h^{r_1\mathbf{d}_1^*}\cdot h^{r_2\mathbf{d}_3^*}K_1^1=h^{r_1w_1\mathbf{d}_1^*}h^{r_1w_2\rho\mathbf{d}_1^*}h^{\alpha\mathbf{d}_1^*}\cdot h^{r_2w_1\mathbf{d}_3^*},K_2^1=h^{r_1w_3\mathbf{d}_1^*}\cdot h^{r_2w_4\mathbf{d}_3^*}h^{r_2w_3\mathbf{d}_3^*}).$$

- 加密 $\mathrm{Enc}(\mathrm{pp},\ \mathrm{mpk},\ \mathrm{ek}_{\sigma},rcv,m)$: 取 $s_1\leftarrow_R\mathbb{Z}_p$, 然后输出:

$$\mathrm{ct}=(C_0=g^{s_1\mathbf{d}_1}\cdot K_0^2,C_1=g^{s_1w_1\mathbf{d}_1}g^{s_1w_2rcv\mathbf{d}_1}\cdot K_1^2,C_2=g^{s_1w_3\mathbf{d}_1}\cdot K_2^2,C_3=e(g^{\mathbf{d}_1},h^{\mathbf{d}_1^*})^{\alpha s_1}\cdot m).$$

- 解密 $\mathrm{Dec}(\mathrm{pp},\mathrm{dk}_{\rho},\mathrm{snd},\mathrm{ct})$: 计算 $m=C_3/\left(e(C_0,K_1^1)\cdot e(C_0,K_2^{1snd})/e(C_1,K_0^1)\cdot e(C_2^{snd},K_0^1)\right)$.

正确性:

$$\begin{aligned}
&e(C_0,K_1^1)\cdot e(C_0,K_2^1snd)/e(C_1,K_0^1)\cdot e(C_2^snd,K_0^1)\\
&=e(g^{(s_1\mathbf{d}_1+s_2\mathbf{d}_3)},h^{(r_1w_1+r_1w_2\rho+\alpha)\mathbf{d}_1^*+r_2w_1\mathbf{d}_3^*})\cdot e(g^{(s_1\mathbf{d}_1+s_2\mathbf{d}_3)},h^{(r_1w_3snd\mathbf{d}_1^*+(r_2w_4snd+r_2w_3snd)d_3^*)})/\\
&e(g^{(s_1w_1+s_1w_2rcv)\mathbf{d}_1+(s_2w_1+s_2w_4)\mathbf{d}_3},h^{r_1\mathbf{d}_1^*+r_2\mathbf{d}_3^*})\cdot e(g^{s_1w_3snd\mathbf{d}_1+s_2w_3snd\mathbf{d}_3},h^{r_1\mathbf{d}_1^*+r_2\mathbf{d}_3^*})\\
&=g_T^{\alpha s_1}.
\end{aligned}$$

5.4 安全性分析

定理 7. 基于 DS 假设, IB-ME 方案 Π_{P2} 满足隐私性和真实性.

证明: 详细证明与合数阶版本 Π_{C1} 对应, 此处予以省略.

5.5 效率分析

对于上文提出的两种方案, 可以计算出如表 1 所示的参数大小以及配对次数, 并与现有唯一 IB-ME 方案 CLWW22 [4]进行对比.

可以看到, 第 1 种方案 Π_{P1} 比现有方案参数更少, 但配对次数略多.

而第 2 种方案 Π_{P2} 不仅有整体参数远小于现有方案, 并改善了配对次数过多的问题, 大大改进了 IB-ME 方案的效率, 提高了实用性.

6 素数阶群上的 IPE-ME

6.1 构造 Π_{IPE}

进一步地, 将 *rcv*-ρ 对的等值策略升级成内积策略, 这意味着当且仅当 $<v,\mathbf{x}>=0$ 时, 属性 v 与策略 $\mathbf{x}$ 匹配. 这样得到的 ME 方案被称为 IPE-ME. 本文的 IPE-ME 方案由 Chen 等人[4] 的方案改良得到. 不失一般性地, $\mathbf{x}$ 中的第 1 个部分 x_1 等于 1.

- $\mathrm{Setup}(\lambda)$: 运行群生成元 $\mathbb{G}=(p,G,H,G_T,e,g,h)\leftarrow\mathcal{G}(\lambda)$, 然后输出 $\mathrm{pp}=\mathbb{G}$.

随机抽取对偶正交基 $(\mathbb{D},\mathbb{D}^*)\leftarrow_R\mathrm{Dual}\left(\mathbb{Z}_p^{2n+2}\right)$. 用 $\mathbf{d}_1,\ldots,\mathbf{d}_{2n+2}$ 表示 $\mathbb{D}$ 的元素, 并用 $\mathbf{d}_1^*,\ldots,\mathbf{d}_{2n+2}^*$ 表示 $\mathbb{D}^*$ 的元素.

令 $g_T = e(g_1, g_2)^{\mathbf{d}_i \cdot \mathbf{d}_i^*}$，取 $\alpha \leftarrow_R \mathbb{Z}_p$，然后输出 $\mathrm{mpk} = (g^{\mathbf{d}_1}, \ldots, g^{\mathbf{d}_n}, g_T^{\alpha})$，储存 $\mathrm{msk} = (g^{\mathbf{d}_{2n+1}}, g^{\mathbf{d}_{2n+2}}, h^{\mathbf{d}_1^*}, \ldots, h^{\mathbf{d}_n^*}, h^{\mathbf{d}_{2n+1}^*}, h^{\mathbf{d}_{2n+2}^*}, \alpha)$.

- SKGen (pp, msk, σ): 取 $r \leftarrow_R \mathbb{Z}_p$, 然后输出 $\mathrm{ek}_\sigma = g^{r(\sigma \mathbf{d}_{2n+1} - \mathbf{d}_{2n+2})}$.
- RKGen (pp, msk, v): 取 $s_1, s_2, s \leftarrow_R \mathbb{Z}_p$, 然后输出:

$$\mathrm{dk}_v = (K_1 = h^{\alpha \mathbf{d}_1^* + s_1(v_1 \mathbf{d}_1^* + \cdots + v_n \mathbf{d}_n^*) + s \mathbf{d}_{2n+1}^*}, K_2 = h^{s_2(v_1 \mathbf{d}_1^* + \cdots + v_n \mathbf{d}_n^*) + s \mathbf{d}_{2n+2}^*}).$$

- Enc(pp, mpk, $\mathrm{ek}_\sigma, \mathbf{x}, m$) : 取 $z \leftarrow_R \mathbb{Z}_p$, 然后输出 $\mathrm{ct} = (C_1 = \mathrm{ek}_\sigma \cdot g^{z(x_1 \mathbf{d}_1 + \ldots + x_n \mathbf{d}_n)}, C_2 = g_T^{\alpha z} \cdot m)$.
- Dec$(\mathrm{pp}, \mathrm{dk}_v, snd, \mathrm{ct})$ ：计算 $m = C_2 \cdot / e(C_1, K_1 \cdot K_2^{snd})$.

正确性:

$$e\left(C_1, K_1 \cdot K_2^{snd}\right) = (g_T)^{\alpha z + s_1 z \sum\limits_{i \in [n]} x_i v_i + s_2 z \cdot snd \sum\limits_{i \in [n]} x_i v_i + \alpha_2 s + r s \sigma - r s \cdot snd} = g_T^{\alpha z}.$$

6.2 安全性分析

定理 8. 基于 DS 假设, IPE-ME 方案满足隐私性和真实性.

证明: 根据上述方案的证明以及 Chen 等人[16] 2012 年的工作中的证明, 定理 8 可证, 此处予以省略.

7 总 结

身份基匹配加密 (IB-ME) 是一种新型的密码学原语, 它允许发送与接收双方均可指定对方的身份, 只有身份匹配时才可以进行通讯. 等值策略的内积匹配加密 (IPE-ME) 是 IB-ME 的升级版, 即策略由等值升级为内积, 扩大发送方的权限.

本文致力于提高现有 IB-ME 方案的效率, 主要贡献如下.

(1) 在标准模型下基于 SXDH 假设, 构造了合数阶群上具有短参数的 IB-ME 方案;

(2) 在标准模型基于相同假设, 在素数阶群上提出了改进的 IB-ME 方案, 保持了短参数的优势, 并且相较于现有的所有方案, 效率最高, 特别是在密文长度和私钥长度方面有显著的改善;

(3) 提出了第 1 个标准模型下等值策略的内积匹配加密方案.

提高 IB-ME 方案的效率有利于促进 IB-ME 方案的进一步应用, 增强实际应用意义.

References:

[1] Ateniese G, Francati D, Nuñez D, Venturi D. Match me if you can: Matchmaking encryption and its applications. Journal of Cryptology, 2021, 34(3): 16. [doi: 10.1007/s00145-021-09381-4]

[2] Balfanz D, Durfee G, Shankar N, Smetters D, Staddon J, Wong HC. Secret handshakes from pairing-based key agreements. In: Proc. of the 2003 Symp. on Security and Privacy. Berkeley: IEEE, 2003. 180–196. [doi: 10.1109/SECPRI.2003.1199336]

[3] Francati D, Guidi A, Russo L, Venturi D. Identity-based matchmaking encryption without random oracles. In: Proc. of the 22nd Int'l Conf. on Cryptology in India on Progress in Cryptology. Jaipur: Springer, 2021. 415–435. [doi: 10.1007/978-3-030-92518-5_19]

[4] Chen J, Li Y, Wen JM, Weng J. Identity-based matchmaking encryption from standard assumptions. In: Proc. of the 28th Int'l Conf. on the Theory and Application of Cryptology and Information Security on Advances in Cryptology. Taipei: Springer, 2022. 394–422. [doi: 10.1007/978-3-031-22969-5_14]

[5] Xu SM, Ning JT, Li YJ, Zhang YH, Xu GW, Huang XY, Deng RH. Match in my way: Fine-grained bilateral access control for secure cloud-fog computing. IEEE Trans. on Dependable and Secure Computing, 2022, 19(2): 1064–1077. [doi: 10.1109/TDSC.2020.3001557]

[6] Xu SM, Ning JT, Ma JH, Huang XY, Pang HH, Deng RH. Expressive bilateral access control for Internet-of-Things in cloud-fog computing. In: Proc. of the 26th ACM Symp. on Access Control Models and Technologies. New York: Association for Computing Machinery, 2021. 143–154. [doi: 10.1145/3450569.3463561]

[7] Nie XY, Yuan Y, Sun JF. Puncturable attribute-based matchmaking encryption scheme. Journal of Cryptologic Research, 2022, 9(5): 883–898 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000555]

[8] Okamoto T, Takashima K. Homomorphic encryption and signatures from vector decomposition. In: Proc. of the 2nd Int'l Conf. on Pairing-Based Cryptography. Egham: Springer, 2008. 57–74. [doi: 10.1007/978-3-540-85538-5_4]

[9] Okamoto T, Takashima K. Hierarchical predicate encryption for inner-products. In: Proc. of the 15th Int'l Conf. on the Theory and Application of Cryptology and Information Security on Advances in Cryptology. Tokyo: Springer, 2009. 214–231. [doi: 10.1007/978-3-

642-10366-7_13]
[10] Chen J, Lim HW, Ling S, Wang HX, Wee H. Shorter identity-based encryption via asymmetric pairings. Designs, Codes and Cryptography, 2014, 73(3): 911–947. [doi: 10.1007/s10623-013-9834-3]
[11] Chen J, Gong JQ, Wee H. Improved inner-product encryption with adaptive security and full attribute-hiding. In: Proc. of the 24th Int'l Conf. on the Theory and Application of Cryptology and Information Security on Advances in Cryptology. Brisbane: Springer, 2018. 673–702. [doi: 10.1007/978-3-030-03329-3_23]
[12] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Proc. of the 27th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology. Istanbul: Springer, 2008. 146–162. [doi: 10.1007/978-3-540-78967-3_9]
[13] Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Proc. of the 29th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology. French Riviera: Springer, 2010. 62–91. [doi: 10.1007/978-3-642-13190-5_4]
[14] Okamoto T, Takashima K. Adaptively attribute-hiding (hierarchical) inner product encryption. In: Proc. of the 31st Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology. Cambridge: Springer, 2012. 591–608. [doi: 10.1007/978-3-642-29011-4_35]
[15] Wee H. Dual system encryption via predicate encodings. In: Proc. of the 11th Int'l Conf. on Theory of Cryptography. San Diego: Springer, 2014. 616–637. [doi: 10.1007/978-3-642-54242-8_26]
[16] Chen J, Lim HW, Ling S, Wang HX, Wee H. Shorter IBE and signatures via asymmetric pairings. In: Proc. of the 5th Int'l Conf. on Pairing-based Cryptography. Cologne: Springer, 2013. 122–140. [doi: 10.1007/978-3-642-36334-4_8]
[17] Chen J, Gay R, Wee H. Improved dual system ABE in prime-order groups via predicate encodings. In: Proc. of the 34th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology. Sofia: Springer, 2015. 595–624. [doi: 10.1007/978-3-662-46803-6_20]
[18] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Proc. of the 2nd Theory of Cryptography Conf. on Theory of Cryptography. Cambridge: Springer, 2005. 325–341. [doi: 10.1007/978-3-540-30576-7_18]
[19] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proc. of the 7th Theory of Cryptography Conf. on Theory of Cryptography. Zurich: Springer, 2010. 455–479. [doi: 10.1007/978-3-642-11799-2_27]
[20] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Proc. of the 29th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2009. 619–636. [doi: 10.1007/978-3-642-03356-8_36]

附中文参考文献:

[7] 聂旭云, 袁玉, 孙剑飞. 可穿刺的基于属性的匹配加密方案. 密码学报, 2022, 9(5): 883–898. [doi: 10.13868/j.cnki.jcr.000555]

陈洁(1985－), 男, 博士, 研究员, 博士生导师, CCF 专业会员, 主要研究领域为公钥密码学.

杜秋妍(2000－), 女, 博士生, 主要研究领域为属性基加密.

楚乔涵(1997－), 女, 博士生, 主要研究领域为属性基加密, 函数加密.

高莹(1977－), 女, 博士, 副教授, 博士生导师, CCF 高级会员, 主要研究领域为隐私计算, 密码学应用.