中国科学: 信息科学 2021 年 第 51 卷 第 6 期: 1013–1029
SCIENTIA SINICA Informationis
论文

CCA 安全的抗泄露 IBE 机制的新型构造

周彦伟[1,2,3], 杨波[1*], 夏喆[4], 张明武[2,3]

1. 陕西师范大学计算机科学学院, 西安 710062
2. 密码科学技术国家重点实验室, 北京 100878
3. 桂林电子科技大学广西可信软件重点实验室, 桂林 541004
4. 武汉理工大学计算机科学与技术学院, 武汉 430070
* 通信作者. E-mail: byang@snnu.edu.cn

收稿日期: 2020–01–02; 修回日期: 2020–02–27; 接受日期: 2020–04–05; 网络出版日期: 2021–05–12

国家重点研发计划 (批准号: 2017YFB0802000)、国家自然科学基金 (批准号: 61802242, 61772326, 61802241)、“十三五” 国家密码发展基金 (批准号: MMJJ20180217)、中央高校基本科研业务费资助项目 (批准号: GK202003079) 和广西可信软件重点实验室研究课题 (批准号: KX202002) 资助

摘要 隐私信息的泄露已成为密码系统当前的严重安全性隐患, 因此抗泄露性将是密码机制必备的安全属性之一. 目前, 通常基于非交互式零知识论证系统、一次性损耗滤波器、强一次性签名等密码基础工具来实现选择密文攻击 (chosen-ciphertext attack, CCA) 安全的抗泄露身份基加密 (identity-based encryption, IBE) 机制的通用构造; 然而, 由于底层工具的计算效率较低, 导致传统通用构造尚未达到理想的计算效率. 针对上述不足, 本文提出一个双封装密钥的身份基哈希证明系统 (identity-based Hash proof system with two encapsulated key, T-IB-HPS) 的新密码学原语, 并详细介绍了 T-IB-HPS 的形式化定义及安全属性; 同时, 基于 T-IB-HPS 和消息验证码 (message authentication code, MAC) 设计了 CCA 安全的抗泄露 IBE 机制的新型通用构造, 并基于 T-IB-HPS 和 MAC 的安全属性, 对通用构造的 CCA 安全性进行了形式化证明; 为进一步展示本文通用构造的实用性, 在 T-IB-HPS 形式化定义的基础上, 我们设计了 T-IB-HPS 的具体实例, 并基于判定的双线性 Diffie-Hellman 假设证明了本文实例的安全性. 相较于传统 CCA 安全的抗泄露 IBE 机制的通用构造而言, 本文通用构造未使用计算效率低的密码学基础工具, 表明了本文的通用构造方法具有较高的计算效率.

关键词 哈希证明系统, 身份基哈希证明系统, 身份基加密机制, 抗泄露攻击

1 引言

传统的密码学机制均在理想的安全模型中对密码机制相应的安全性进行了证明, 在该理想安全模型中均假设任意的敌手仅能接触密码机制特定的输入和输出, 无法获知密码机制运行过程的任何秘密

引用格式: 周彦伟, 杨波, 夏喆, 等. CCA 安全的抗泄露 IBE 机制的新型构造. 中国科学: 信息科学, 2021, 51: 1013–1029, doi: 10.1360/SSI-2020-0001
Zhou Y W, Yang B, Xia Z, et al. A new construction of leakage-resilient CCA secure IBE scheme (in Chinese). Sci Sin Inform, 2021, 51: 1013–1029, doi: 10.1360/SSI-2020-0001

© 2021《中国科学》杂志社

信息, 如随机数、用户私钥等. 然而, 现实环境中往往存在各种各样的物理攻击 (如边信道、冷启动等) 导致敌手能够获得密码机制运行过程中秘密信息的部分泄露, 使得传统理想安全模型下可证明安全的密码机制, 在现实环境中由于泄露的存在已不再满足其所声称的安全性. 为了增强密码机制的实用性, 提升其抵抗泄露攻击的能力, 需进一步研究存在信息泄露环境下安全密码机制的设计.

近年来, 为了缩短实际应用与理论研究之间的差距, 抗泄露密码学的研究已引起密码学研究者的广泛关注, 即在秘密信息存在部分泄露的前提下, 设计仍然保持安全的密码机制. 由此可见, 设计更接近于现实环境的抗泄露密码机制已成为当前密码学研究领域的热点问题之一. 此外, 虽然通用构造的设计难度较大, 但实用性更强, 并且具有更优的推广性, 因此研究者倾向于设计密码机制抗泄露攻击的通用构造形式.

1.1 泄露容忍性的研究现状

Naor 和 Segev [1] 分别提出了泄露容忍的选择明文攻击 (leakage-resilient chosen plaintext attacks, LR-CPA) 安全性和泄露容忍的选择密文攻击 (leakage-resilient chosen ciphertext attacks, LR-CCA) 安全性, 并基于哈希证明系统 (Hash proof system, HPS) 和强随机性提取器 (strong randomness extractor, Ext) 设计了抵抗有界泄露攻击的公钥加密 (public-key encryption, PKE) 机制的通用构造方法; 但是, 上述通用构造仅实现了选择明文攻击 (chosen plaintext attacks, CPA) 的安全性. 然而, 对于一个加密机制而言, 选择密文攻击 (chosen ciphertext attacks, CCA) 安全性是一个非常实用且重要的安全属性. 因此, 为进一步提高抗泄露 PKE 机制的实用性, Qin 等 [2,3] 基于 HPS 和一次性损耗滤波器 (one-time lossy filter, OT-LF) 给出了具有 LR-CCA 安全性的 PKE 机制的通用构造, 并且针对该通用构造方法提出了相应的实例. 特别地, 传统 PKE 机制实现 CCA 安全性的方法通常有两种: (1) CPA 安全的 PKE 机制结合非交互式零知识证明 (non-interactive zero-knowledge, NIZK) 系统; (2) 基于平滑的 HPS 构造. 此外, Canetti 等 [4] 提出了基于较弱的选择安全性身份基加密 (identity-based encryption, IBE) 机制和强一次性签名构造 CCA 安全的 PKE 机制的通用方法 (简称 CHK 转换); 类似地, 基于该方法也可以通过抗泄露的 IBE 机制构造抗泄露的 PKE 机制. 然而, Boneh 和 Katz [5] 指出 CHK 转换尚未达到最佳的计算效率, 同时, 提出了相应的改进方法 (简称 BK 转换). 由于连续泄露模型中敌手能够进行持续的泄露攻击, 使得连续泄露容忍的密码机制更加接近现实环境的实际应用需求, 并且在 FOCS2010 中, Dodis 等 [6] 详细介绍了连续泄露模型中的敌手攻击能力的定义, 同时给出了连续泄露模型与有界泄露模型间的转换联系.

Alwen 等 [7] 将 HPS 的概念扩展到基于身份的密码学中, 提出了一个新的密码学原语 – 身份基哈希证明系统 (identity-based Hash proof system, IB-HPS), 并基于 IB-HPS 和强随机性提取器提出了 CPA 安全的抗泄露 IBE 机制的通用构造方法. 为了设计抵抗连续泄露攻击的 IBE 机制, Zhou 等 [8] 提出了可更新的身份基哈希证明系统 (updatable identity-based Hash proof system, U-IB-HPS) 的新密码学原语, 并基于该技术设计了 IBE 机制、基于身份的混合加密机制和基于身份的密钥协商协议等密码系统抗泄露版本的通用构造方法; 并设计了具有匿名性的 U-IB-HPS 来构造匿名的抗泄露 IBE 机制 [9]. 最近, 为了设计性能更优的 U-IB-HPS, 文献 [10] 基于向量正交技术提出一个新的 U-IB-HPS 的具体构造, 该机制具有更加完美的秘钥更新功能. 文献 [11] 以 IB-HPS、对称加密机制和强一次性签名机制 (one-time signature, OTS) 为基础工具提出了一个新的 CCA 安全的抗泄露 IBE 机制的通用构造.

1.2 我们的思路

现有抗泄露 IBE 机制的通用构造方法总结如表 1 所示. 分析可知, 为了实现 CCA 安全性, 现有

表 1 与现有抗 (连续) 泄露 CCA 安全 IBE 机制通用构造方法的比较

Table 1 Comparison with the generic construction of previous (continuous) leakage-resilient CCA secure IBE scheme

	Previous method	Our method
Bounded leakage resilience	IB-HPS+Ext+OT-LF (NIZK)	T-IB-HPS+Ext+MAC
Continuous leakage resilience	U-IB-HPS+Ext+OT-LF (NIZK)	U-T-IB-HPS+Ext+MAC

方法使用了 NIZK, OT-LF 和 OTS 等计算效率较低的密码学工具, 导致相应密码机制通用构造的计算效率较低. 为了提高通用构造的计算效率, 底层应使用计算效率较高的基础密码学工具来构造 CCA 安全的 IBE 机制. 虽然, Boneh 和 Katz [5] 在 CHK 转换 [4] 的基础上, 基于消息验证码和封装机制提出了效率更高的 CCA 安全的 PKE 机制的通用构造方法; 然而该方法无法直接迁移到抗泄露 IBE 机制的构造中, 因为 IB-HPS 输出的封装密钥用来完成对明文消息的加密, 无法参与到消息验证码的计算中来确保密文标签的合法性. 此外, 文献 [11] 中的构造使用了对称加密和一次性签名机制, 计算效率较传统方法是有所提升, 但并非是最佳的构造方案.

为了设计更加高效的 CCA 安全的抗泄露 IBE 机制的通用构造, 本文在 IB-HPS 的基础上, 提出了一个新的密码学原语, 称为双封装密钥的身份基哈希证明系统 (identity-based Hash proof system with two encapsulated key, T-IB-HPS), 并且定义了该系统相应的安全属性, 如正确性、通用性、平滑性和有效封装密文与无效封装密文的不可区分性等. 在 CCA 安全的抗泄露 IBE 机制的通用构造中, 底层 T-IB-HPS 的封装算法在输出封装密文的同时输出了两个互不相同的封装密钥, 其中一个完成对明文消息的加密, 另一个作为消息验证码 (message authentication code, MAC) 的对称密钥对输入消息产生相应的标签, 实现密文的防扩展性. 本文方法与现有技术的对比如表 1 所述.

1.3 我们的工作

相较于现有 CCA 安全的抗泄露 IBE 机制的通用构造, 我们的构造方法具有更高的计算效率. 本文的贡献主要分为以下 3 个方面:

(1) 提出了一个新的密码学原语 – 双封装密钥的身份基哈希证明系统 (T-IB-HPS), 并且定义了相应的安全属性, 如正确性、通用性、(泄露) 平滑性和有效封装密文与无效封装密文的不可区分性等.

(2) 基于泄露平滑的 T-IB-HPS 和 MAC 设计了高效 CCA 安全的抗泄露 IBE 机制的通用构造, 并基于底层 T-IB-HPS 和 MAC 的安全性证明了上述通用构造的 CCA 安全性; 此外, 底层泄露平滑的 T-IB-HPS 确保了上层通用构造的抗泄露性.

(3) 为展示抗泄露 IBE 机制通用构造的实用性, 本文设计了一个 T-IB-HPS 的具体实例, 并基于判定的双线性 Diffie-Hellman (decisional bilinear Diffie-Hellman, DBDH) 假设在选择身份安全模型下对有效封装密文与无效封装密文的不可区分性进行了形式化证明.

2 基础知识

本文用 κ 表示安全参数, $a \leftarrow_R A$ 表示从集合 A 中均匀随机的选取元素 a, $\mathsf{negl}(\kappa)$ 表示在安全参数 κ 上是计算可忽略的, $a \leftarrow A(b)$ 表示算法 A 在输入 b 的作用下输出相应的计算结果 a; 此外, PPT 是概率多项式时间 (probabilistic polynomial time) 的缩写.

2.1 强随机性提取器

定义1 (统计距离) 有限域 Ω 上任意两个随机变量 A 与 B 间的统计距离可表示为

$$\mathsf{SD}(A,B)=\frac{1}{2}\sum_{w\in\Omega}\big|\Pr[A=w]-\Pr[B=w]\big|.$$

定义2 (最小熵) 设 A 是确定的随机变量, 则变量 A 的最小熵可表示为

$$H_\infty(A)=-\log(\max_a\Pr[A=a]).$$

定义3 (平均最小熵) 当变量 B 已知时, 变量 A 的平均最小熵可表示为

$$\widetilde{H}_\infty(A|B)=\log(\mathrm{E}_z\max_a\Pr[A=a|B=b])=-\log(\mathrm{E}_{b\leftarrow B}[2^{-H_\infty(A|B=b)}]),$$

其中 E 表示数学期望运算.

定理1 对于任意的随机变量 A, B 和 C, 若 B 的取值最多有 2^l 个, 则有 $\widetilde{H}_\infty(A|(B,C))\geqslant\widetilde{H}_\infty(A|C)-l$.

定义4 (强随机性提取器) 令随机变量 A 和 B 满足条件 $A\in\{0,1\}^{l_n}$ 和 $\widetilde{H}_\infty(A|B)\geqslant k$, 对于任意的 $S\in\{0,1\}^{l_t}$ 和 $C\in\{0,1\}^{l_m}$, 若有 $\mathsf{SD}((\mathsf{Ext}(A,S),S,B),(C,S,B))$ 成立, 则称函数 $\mathsf{Ext}:\{0,1\}^{l_n}\times\{0,1\}^{l_t}\to\{0,1\}^{l_m}$ 是平均情况的 (k,ε) – 强随机性提取器, 其中 $S\in\{0,1\}^{l_t}$ 是可公开的提取器种子.

2.2 困难性假设

定义5 (判定的双线性 Diffie-Hellman 假设) 对于 $(p,g,G,G_T,e(\cdot))\leftarrow\mathcal{G}(1^\kappa)$, 其中 G 和 G_T 是阶为大素数 p 的循环群, g 是群 G 的生成元, $e:G\times G\to G_T$ 是双线性映射. 给定元组 $(g,g^a,g^b,g^c,e(g,g)^{abc})$ 和 $(g,g^a,g^b,g^c,e(g,g)^d)$, 对于任意未知的指数 $a,b,c,d\leftarrow_R Z_p^*$, DBDH 问题的目标是判断 $e(g,g)^{abc}=e(g,g)^d$ 是否成立. DBDH 假设意味着任意的 PPT 算法成功解决 DBDH 问题的优势

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DBDH}}(\kappa)=|\Pr[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^d)=1]|$$

是可忽略的, 其中概率来源于 a,b,c,d 在 Z_p^* 上的随机选取和算法 $\mathcal{A}$ 的随机选择.

特别地, $e(g,g)^d$ 是群 G_T 中的任意元素, 本文中为了方便证明的描述, 将 $e(g,g)^d$ 用 $e(g,g)^{abc'}$ 替换, 其中 $c'\leftarrow_R Z_p^*$ 且 $c'\neq c$.

2.3 消息验证码

密钥空间 $\mathcal{K}$ 和消息空间 $\mathcal{M}$ 上的消息验证码 $\mathsf{MAC}=(\mathsf{Tag},\mathsf{Ver})$ 包含以下两个算法:

(1) $\mathsf{Tag}(k,m)$: 输入密钥空间中的对称密钥 $k\in\mathcal{K}$ 和消息空间中的消息 $m\in\mathcal{M}$, 标签算法 Tag 输出一个认证标签 Tag.

(2) $\mathsf{Ver}(k,m,\mathrm{Tag})$: 输入密钥空间中的对称密钥 $k\in\mathcal{K}$、消息空间中的消息 $M\in\mathcal{M}$ 和认证标签 Tag, 验证算法 Ver 输出相应的验证结果 0 或 1, 其中 1 表示 Tag 是关于消息 M 的认证标签, 否则输出 0.

消息验证码 $\mathsf{MAC}=(\mathsf{Tag},\mathsf{Ver})$ 的正确性要求, 对于密钥空间 $\mathcal{K}$ 上任意的对称密钥 $k\in\mathcal{K}$, 有

$$\mathsf{Ver}(k,M,\mathsf{Tag}(k,M))=1$$

成立. 消息验证码 $\mathsf{MAC}=(\mathsf{Tag},\mathsf{Ver})$ 的安全性通过下述交互式实验 $\mathsf{Exp}_{\mathrm{MAC}}^{\text{suf-cmva}}(\kappa)$ 来描述:

(1) 从密钥空间 $\mathcal{K}$ 中随机选取对称密钥 $k\in\mathcal{K}$.

(2) 运行 $\mathcal{A}^{\mathsf{Tag}(k,\cdot),\mathsf{Ver}(k,\cdot,\cdot)}(\kappa)$, 其中 $\mathsf{Tag}(k,\cdot)$ 是标签谕言机, 敌手 $\mathcal{A}$ 能够从它获得相应消息的认证标签; $\mathsf{Ver}(k,\cdot,\cdot)$ 是验证谕言机, 敌手 $\mathcal{A}$ 能从它获得消息及相应标签的验证结果.

(3) 敌手 $\mathcal{A}$ 输出一个挑战消息标签对 (m^*,Tag^*), 并且 (m^*,Tag^*) 与之前标签谕言机 $\mathsf{Tag}(k,\cdot)$ 返回的所有值 (m_i,Tag_i) 均不相同. 若有 $\mathsf{Ver}(k,m^*,\mathrm{Tag}^*)=1$ 成立, 则输出 1, 否则输出 0.

特别地, 由于 $(m^*,\mathrm{Tag}^*)\neq(m^*,\mathrm{Tag}')$, 则元组 (m^*,Tag') 可以出现在标签谕言机 $\mathsf{Tag}(k,\cdot)$ 的返回值列表中, 即敌手 $\mathcal{A}$ 可以对挑战消息 m^* 进行标签生成询问. 敌手 $\mathcal{A}$ 在上述交互式实验 $\mathsf{Exp}_{\mathrm{MAC}}^{\text{suf-cmva}}(\kappa)$ 中获胜的优势定义为 $\mathsf{Adv}_{\mathrm{MAC}}^{\text{suf-cmva}}(\kappa)=|\Pr[\mathsf{Exp}_{\mathrm{MAC}}^{\text{suf-cmva}}(\kappa)=1]|$.

定义6 (消息验证码的强不可伪造性) 对于任意的 PPT 敌手 $\mathcal{A}$, 若有 $\mathsf{Adv}_{\mathrm{MAC}}^{\text{suf-cmva}}(\kappa)\leqslant\mathsf{negl}(\kappa)$ 成立, 那么该消息验证码 $\mathsf{MAC}=(\mathsf{Tag},\mathsf{Ver})$ 在选择消息和选择验证询问攻击下是强不可伪造的.

3 抗泄露的 IBE 机制

本节将回顾 IBE 机制的形式化定义和抗泄露的安全性模型. 关于抗泄露 IBE 机制的定义及安全性的更多介绍详见文献 [12∼14].

3.1 形式化定义

一个 IBE 机制包含 4 个 PPT 算法 Setup, KeyGen, Enc 和 Dec. 各算法的具体描述如下所述:

(1) $(\mathrm{Params},\mathrm{msk})\leftarrow\mathsf{Setup}(1^\kappa)$. 初始化算法 Setup 以系统安全参数 κ 为输入, 输出相应的系统公开参数 Params 和主密钥 msk, 其中 Params 定义了身份空间 $\mathcal{ID}$, 私钥空间 $\mathcal{SK}$ 和密文空间 $\mathcal{M}$. 此外, Params 是其他算法 KeyGen、Enc 和 Dec 的隐含输入; 为了方便, 下述算法的输入并未将其列出.

(2) $\mathrm{sk}_{\mathrm{id}}\leftarrow\mathsf{KeyGen}(\mathrm{msk},\mathrm{id})$. 输入任意身份 $\mathrm{id}\in\mathcal{ID}$ 和主密钥 msk, 密钥生成算法 KeyGen 输出身份 id 所对应的私钥 $\mathrm{sk}_{\mathrm{id}}$.

(3) $C\leftarrow\mathsf{Enc}(\mathrm{id},M)$. 对于输入的身份 $\mathrm{id}\in\mathcal{ID}$ 和明文消息 $M\in\mathcal{M}$, 加密算法 Enc 输出身份 id 对消息 M 的加密密文 C.

(4) $M\leftarrow\mathsf{Dec}(\mathrm{sk}_{\mathrm{id}},C)$. 输入密文 C 和身份 id 所对应的私钥 $\mathrm{sk}_{\mathrm{id}}$, 解密算法 Dec 输出相应的明文消息 M.

3.2 安全模型

在泄露环境下, 通过赋予敌手访问泄露谕言机 $\mathcal{O}_{\mathrm{sk}_{\mathrm{id}}}^{\lambda,\kappa}(\cdot)$ 的能力来模拟敌手的泄露攻击, 访问时敌手需提交高效可计算的泄露函数 $f_i:\{0,1\}^*\rightarrow\{0,1\}^{\lambda_i}$ 给 $\mathcal{O}_{\mathrm{sk}_{\mathrm{id}}}^{\lambda,\kappa}(\cdot)$.

定义7 (泄露谕言机) 泄露谕言机 $\mathcal{O}_{\mathrm{sk}_{\mathrm{id}}}^{\lambda,\kappa}(\cdot)$ 的参数包括安全参数 κ, 系统设定的泄露界 λ 和相应身份的私钥 $\mathrm{sk}_{\mathrm{id}}$, 当收到敌手提交的多项式时间内高效可计算的泄露函数 $f_i:\{0,1\}^*\rightarrow\{0,1\}^{\lambda_i}$ 后, 谕言机 $\mathcal{O}_{\mathrm{sk}_{\mathrm{id}}}^{\lambda,\kappa}(\cdot)$ 计算并返回相应的泄露信息 $f_i(\mathrm{sk}_{\mathrm{id}})$ 给敌手, 但所有询问中, 同一私钥 $\mathrm{sk}_{\mathrm{id}}$ 的泄露总量不能超过泄露参数 λ, 即 $\sum_{i=1}^{t}f_i(\mathrm{sk}_{\mathrm{id}})\leqslant\lambda$, 其中 t 表示泄露询问的总次数; 否则将返回特殊符号 $\perp$ 给敌手.

IBE 机制泄露容忍的 CCA 安全性游戏由模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 执行, 其中 κ 是安全参数, λ 是泄露参数. 特别地, 与现有工作 [12∼17] 相类似, 本文仅考虑挑战之前的泄露. 也就是说, 敌手获得挑战密文之后将不能进行泄露询问.

模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 间消息交互的具体过程如下所述:

(1) 初始化. 模拟器 $\mathcal{S}$ 输入安全参数 κ, 运行初始化算法 $\mathsf{Setup}(1^\kappa)$, 产生公开的系统参数 Params 和保密的主密钥 msk, 发送 Params 给敌手 $\mathcal{S}$.

(2) 阶段 1 (训练). 在该阶段敌手 $\mathcal{A}$ 适应性地进行多项式有界次的下述询问:

密钥生成询问. 对于身份 id 的密钥生成询问, 模拟器 $\mathcal{S}$ 运行密钥生成算法 KeyGen, 返回相应的用户私钥 $\mathrm{sk_{id}}$ 给敌手 $\mathcal{A}$.

解密询问. 对于身份和密文二元组 (id, C) 的解密询问, 模拟器 $\mathcal{S}$ 运行密钥生成算法 KeyGen, 产生身份 id 所对应的私钥 $\mathrm{sk_{id}}$, 再运行解密算法 Dec, 用 $\mathrm{sk_{id}}$ 解密密文 C, 并将相应的明文 M 发送给 $\mathcal{A}$.

泄露询问. 对于身份 id 对应私钥的泄露询问, 模拟器 $\mathcal{S}$ 运行密钥生成算法 KeyGen, 产生身份 id 对应的密钥 $\mathrm{sk_{id}}$, 再运行泄露谕言机 $\mathcal{O}^{\lambda,\kappa}_{\mathrm{sk_{id}}}(\cdot)$, 产生密钥 $\mathrm{sk_{id}}$ 的泄露信息 $f_i(\mathrm{sk_{id}})$, 并把 $f_i(\mathrm{sk_{id}})$ 发送给敌手 $\mathcal{A}$, 其中 $f_i : \{0,1\}^* \to \{0,1\}^{\lambda_i}$ 是高效可计算的泄露函数; 但是在整个泄露询问过程中关于同一密钥 $\mathrm{sk_{id}}$ 泄露信息的总量不能超过系统设定的泄露界 λ; 否则 $\mathcal{S}$ 将输出终止符号 $\perp$ 给敌手 $\mathcal{A}$.

(3) 挑战. 敌手 $\mathcal{A}$ 输出两个长度相等的明文 $M_0, M_1 \in \mathcal{M}$ 和一个挑战身份 $\mathrm{id}^* \in \mathcal{ID}$, 限制是挑战身份 id^* 不能在阶段 1 中的任何密钥生成询问中出现, 并且 id^* 对应私钥 $\mathrm{sk_{id^*}}$ 的泄露总量不能超过系统设定的泄露界 λ. 模拟器 $\mathcal{S}$ 选取随机值 $v \leftarrow \{0,1\}$, 计算挑战密文 $C^*_v = \mathsf{Enc}(\mathrm{id}^*, M_v)$, 并将 C^*_v 发送给 $\mathcal{A}$.

(4) 阶段 2 (训练). 该阶段敌手可进行多项式有界次的下述询问.

密钥生成询问. 对身份空间 $\mathcal{ID}$ 中除挑战身份 id^* 之外的任何身份 id ($\mathrm{id} \neq \mathrm{id}^*$) 进行密钥生成询问. 模拟器 $\mathcal{S}$ 以阶段 1 中的方式进行应答.

解密询问. 对除挑战身份和挑战密文之外的身份密文对 (id, C) 的解密询问, 其中 $(\mathrm{id}, C) \neq (\mathrm{id}^*, C^*_v)$. 模拟器 $\mathcal{S}$ 以阶段 1 中的方式进行应答.

(5) 猜测. 敌手 $\mathcal{A}$ 输出对随机数 v 的猜测 v', 如果 $v' = v$, 则敌手 $\mathcal{A}$ 攻击成功.

敌手 $\mathcal{A}$ 在上述游戏中获胜的优势定义为 $\mathsf{Adv}^{\text{LR-CCA}}_{\text{IBE},\mathcal{A}}(\kappa) = |\Pr[v' = v] - \frac{1}{2}|$, 其中概率来自于模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 对随机数的使用.

定义8 (IBE 机制泄露容忍的 CCA 安全性) 若对任意的 PPT 敌手 $\mathcal{A}$, 其在上述游戏中获胜的优势 $\mathsf{Adv}^{\text{LR-CCA}}_{\text{IBE},\mathcal{A}}(\kappa)$ 是可忽略的, 那么相应的 IBE 机制具有泄露容忍的选择密文攻击安全性.

类似地, 在抗泄露 IBE 机制的 CPA 安全性游戏中, 敌手能够执行除解密询问之外的其他询问, 即敌手不具有进行解密询问的能力, 并且对其他询问的限制条件与 CCA 安全性游戏相一致.

4 双封装密钥的身份基哈希证明系统

本节基于传统 IB-HPS [7] 的形式化定义及安全属性等基础知识, 将提出新密码学原语 T-IB-HPS 的形式化定义及安全属性.

4.1 形式化定义

一个 T-IB-HPS 包含 5 个 PPT 算法 Setup, KeyGen, Encap, Encap* 和 Decap. 具体描述如下所述:

(1) $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$. 初始化算法 Setup 以系统安全参数 κ 为输入, 输出相应的系统公开参数 mpk 和主密钥 msk, 其中 mpk 定义了系统的用户身份空间 $\mathcal{ID}$, 封装密钥空间 $\mathcal{K}_1 \times \mathcal{K}_2$, 封装密

文空间 $\mathcal{C}$ 和用户私钥空间 $\mathcal{SK}$. 此外, mpk 是其他算法 KeyGen, Encap, Encap* 和 Decap 的隐含输入; 为了方便起见, 下述算法的输入并未将其列出.

(2) $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$. 对于输入的任意身份 id, 密钥生成算法 KeyGen 以主密钥 msk 作为输入, 输出身份 id 所对应的私钥 $\mathrm{sk}_{\mathrm{id}}$. 特别地, 每次运行该算法, 概率性的密钥生成算法基于不同随机数为用户生成相应的私钥.

(3) $(C, k_1, k_2) \leftarrow \mathsf{Encap}(\mathrm{id})$. 对于输入的任意身份 id, 有效密文封装算法 Encap 输出相应的封装密文 $C \in \mathcal{C}$ 和封装密钥对 $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$, 并且 k_1 和 k_2 满足 $k_1 \neq k_2$. 特别地, 实际构造中封装密钥空间 $\mathcal{K}_1$ 和 $\mathcal{K}_2$ 可以是相同的空间, 但输出的封装密钥 k_1 和 k_2 是互不相同的.

(4) $C^* \leftarrow \mathsf{Encap}^*(\mathrm{id})$. 对于输入的任意身份 id, 无效密文封装算法 Encap* 输出相应的无效封装密文 $C^* \in \mathcal{C}$.

(5) $(k_1', k_2') \leftarrow \mathsf{Decap}(d_{\mathrm{id}}, C)$. 对于确定性的解封装算法, 输入身份 id 所对应的封装密文 C (或 C^*) 和私钥 d_{id}, 输出相应的解封装结果 (k_1', k_2'). 特别地, 解封装算法对于输入的任意密文 (可能是有效密文 C, 也有可能是无效密文 C^*), 均输出相应的解封装结果 k_1' 和 k_2', 且 $(k_1', k_2') \in \mathcal{K}_1 \times \mathcal{K}_2$.

4.2 安全性

一个 T-IB-HPS 需满足正确性、通用性、平滑性及有效封装密文与无效封装密文的不可区分性.

4.2.1 正确性

对于任意的身份 $\mathrm{id} \in \mathcal{ID}$, 有

$$\Pr[k_1' \neq k_1 \cup k_2' \neq k_2 | (C, k_1, k_2) \leftarrow \mathsf{Encap}(\mathrm{id}), (k_1', k_2') \leftarrow \mathsf{Decap}(d_{\mathrm{id}}, C)] \leqslant \mathsf{negl}(\kappa)$$

成立, 其中 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$ 和 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{msk}, \mathrm{id})$.

4.2.2 通用性

对于 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$ 和任意的身份 $\mathrm{id} \in \mathcal{ID}$, 当一个 T-IB-HPS 满足下属两个性质时, 称该 T-IB-HPS 是 δ – 通用的.

- 对于 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$, 有 $H_\infty(d_{\mathrm{id}}) \geqslant \delta$.
- 对于身份 id 对应的任意两个不同的私钥 d_{id}^1 和 d_{id}^2 $(d_{\mathrm{id}}^1 \neq d_{\mathrm{id}}^2)$, 有

$$\Pr[\mathsf{Decap}(C^*, d_{\mathrm{id}}^1) = \mathsf{Decap}(C^*, d_{\mathrm{id}}^2)] \leqslant \mathsf{negl}(\kappa),$$

其中 $C^* \leftarrow \mathsf{Encap}^*(\mathrm{id})$. 由于 T-IB-HPS 的密钥生成算法是概率性算法, 对同一身份多次执行该算法将产生各不相同的私钥.

通用性表明 T-IB-HPS 的用户私钥具有一定的不可预测性; 并且对于同一身份的不同私钥解封装同一个无效密文得到相同解封装结果的概率是可忽略的. 也就是说, 身份所对应的一个无效密文用与该身份相对应的不同私钥去解封装, 将得到互不相同的解封装结果.

4.2.3 平滑性

对于任意身份 $\mathrm{id} \in \mathcal{ID}$ 的私钥 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$, 若有

$$\mathsf{SD}((C^*, k_1', k_2'), (C^*, \hat{k}_1, \hat{k}_2)) \leqslant \mathsf{negl}(\kappa)$$

成立, 则称该 T-IB-HPS 是平滑的, 其中 $C^* \leftarrow \mathsf{Encap}^*(\mathrm{id})$, $(k_1', k_2') \leftarrow \mathsf{Decap}(d_{\mathrm{id}}, C^*)$ 和 $(\hat{k}_1, \hat{k}_2) \leftarrow_R \mathcal{K}_1 \times \mathcal{K}_2$. 平滑性表明无效封装密文的解封装输出结果与封装密钥空间中的任意随机值是不可区分的. 换句话讲, 无效密文的解封装结果对任意敌手而言是完全均匀随机的.

在平滑性的基础上, 下面讨论泄露平滑性. 令函数 $f: \{0,1\}^* \to \{0,1\}^\lambda$ 是一个高效可计算的泄露函数, 若有关系

$$\mathsf{SD}((C^*, f(d_{\mathrm{id}}), k_1', k_2'), (C^*, f(d_{\mathrm{id}}), \hat{k}_1, \hat{k}_2)) \leqslant \mathsf{negl}(\kappa)$$

成立, 则称相应的 T-IB-HPS 具有抗泄露攻击的平滑性, 简称泄露平滑的 T-IB-HPS.

4.2.4 有效封装密文与无效封装密文的不可区分性

有效封装算法 Encap 生成的密文称为有效封装密文, 无效封装算法 Encap^* 输出的密文称为无效封装密文. 对于 T-IB-HPS 而言, 有效封装密文与无效封装密文是不可区分的, 即使敌手能够获得任意身份 (包括挑战身份) 的用户私钥. 有效封装密文与无效封装密文的不可区分性游戏包括挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 两个参与者, 具体的消息交互过程如下所示:

• **初始化.** 挑战者 $\mathcal{C}$ 运行初始化算法 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$, 发送系统公开参数 mpk 给敌手 $\mathcal{A}$, 并秘密保存主私钥 msk.

• **阶段 1.** 敌手 $\mathcal{A}$ 能够适应性的对身份空间 $\mathcal{ID}$ 中的任意身份 $\mathrm{id} \in \mathcal{ID}$ 进行密钥生成询问 (包括挑战身份), 挑战者 $\mathcal{C}$ 通过运行密钥生成算法 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$ 返回相应的私钥 d_{id} 给敌手 $\mathcal{A}$.

• **挑战.** 对于挑战身份 id^*, 挑战者 $\mathcal{C}$ 首先计算 $(C_1, k_1, k_2) \leftarrow \mathsf{Encap}(\mathrm{id}^*)$ 和 $C_0 \leftarrow \mathsf{Encap}^*(\mathrm{id}^*)$, 然后, 发送挑战密文 C_v 给敌手 $\mathcal{A}$, 其中 $v \leftarrow_R \{0,1\}$.

• **阶段 2.** 与阶段 1 相类似, 敌手 $\mathcal{A}$ 能够适应性的对任意身份 $\mathrm{id} \in \mathcal{ID}$ 进行秘钥生成询问 (包括挑战身份), 挑战者 $\mathcal{C}$ 返回相应的私钥 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$ 给敌手 $\mathcal{A}$.

• **输出.** 敌手 $\mathcal{A}$ 输出对 v 的猜测 v'. 若 $v' = v$, 则称敌手 $\mathcal{A}$ 在该游戏中获胜, 并且挑战者 $\mathcal{C}$ 输出 $\omega = 1$, 意味着 $\mathcal{C}$ 能够区分有效密文和无效密文; 否则, 挑战者 $\mathcal{C}$ 输出 $\omega = 0$.

在上述有效封装密文与无效封装密文的区分性实验中, 敌手 $\mathcal{A}$ 获胜的优势定义为

$$\mathsf{Adv}^{\text{VI-IND}}_{\text{T-IB-HPS}}(\kappa) = \left| \Pr[\mathcal{A} \text{ wins}] - \frac{1}{2} \right|,$$

其中概率来自挑战者和敌手对随机数的选取. T-IB-HPS 有效封装密文与无效封装密文的不可区分性要求对于任意的 PPT 敌手 $\mathcal{A}$, 有 $\mathsf{Adv}^{\text{VI-IND}}_{\text{T-IB-HPS}}(\kappa) \leqslant \mathsf{negl}(\kappa)$ 成立.

4.2.5 通用性、平滑性及泄露平滑性之间的关系

下面将讨论通用性、平滑性及泄露平滑性之间的关系, 其中定理 2 表明当参数满足相应的限制条件时任意一个通用的 IB-HPS 是泄露平滑的; 定理 3 表明基于平均情况的强随机性提取器可将平滑的 IB-HPS 转变成泄露平滑的 IB-HPS.

定理2 假设封装密钥空间为 $\mathcal{K}_1 \times \mathcal{K}_2 = \{0,1\}^{l_1} \times \{0,1\}^{l_2}$ 的 T-IB-HPS 是 δ – 通用的, 那么它也是泄露平滑的, 其中泄露参数满足 $\lambda \leqslant \delta - l_1 - l_2 - \omega(\log \kappa)$.

定理 2 可由剩余哈希引理和广义剩余哈希引理得到 [8].

下面基于平均情况的强随机性提取器给出由平滑的 T-IB-HPS 构造泄露平滑的 T-IB-HPS 的通用转换方法. 令 $\Pi' = (\mathsf{Setup}', \mathsf{KeyGen}', \mathsf{Encap}', \mathsf{Encap}'^*, \mathsf{Decap}')$ 是封装密钥空间为 $\mathcal{K}_1' \times \mathcal{K}_2' = \{0,1\}^{l_1'} \times \{0,1\}^{l_2'}$, 身份空间为 $\mathcal{ID}$ 的平滑性 T-IB-HPS; 令 $\mathsf{Ext}_1 : \{0,1\}^{l_1'} \times \{0,1\}^{l_t} \to \{0,1\}^{l_1}$ 是平均情况的

$(l'_1-\lambda,\varepsilon_1)$ – 强随机性提取器, $\mathsf{Ext}_2:\{0,1\}^{l'_2}\times\{0,1\}^{l_t}\to\{0,1\}^{l_2}$ 是平均情况的 $(l'_2-\lambda,\varepsilon_2)$ – 强随机性提取器, 其中 λ 是泄露参数, ε_1 和 ε_2 在安全参数 κ 上是可忽略的. 那么, 泄露平滑的 T-IB-HPS 的构造 $\Pi=(\mathsf{Setup},\mathsf{KeyGen},\mathsf{Encap},\mathsf{Encap}^*,\mathsf{Decap})$ 可表述如下:

• $(\mathrm{mpk},\mathrm{msk})\leftarrow\mathsf{Setup}(1^\kappa)$.

输出 $(\mathrm{mpk},\mathrm{msk})$, 其中 $(\mathrm{mpk},\mathrm{msk})\leftarrow\mathsf{Setup}'(1^\kappa)$.

• $d_{\mathrm{id}}\leftarrow\mathsf{KeyGen}(\mathrm{id},\mathrm{msk})$.

输出 d_{id}, 其中 $d_{\mathrm{id}}\leftarrow\mathsf{KeyGen}'(\mathrm{id},\mathrm{msk})$.

• $(C,k_1,k_2)\leftarrow\mathsf{Encap}(\mathrm{id})$.

计算 $(C',\hat{k}_1,\hat{k}_2)\leftarrow\mathsf{Encap}'(\mathrm{id})$. 随机选取 $S_1,S_2\leftarrow_R\{0,1\}^{l_t}$, 并计算 $k'_1=\mathsf{Ext}_1(\hat{k}_1,S_1)$ 和 $k'_2=\mathsf{Ext}_1(\hat{k}_2,S_2)$. 最后输出封装密文 $C=(C',S_1,S_2)$ 和相应的封装密钥 (k_1,k_2).

• $C^*\leftarrow\mathsf{Encap}^*(\mathrm{id})$.

随机选取 $S_1,S_2\leftarrow_R\{0,1\}^{l_t}$, 并计算 $C^*\leftarrow\mathsf{Encap}'^*(\mathrm{id})$. 输出封装密文 $C^*=(C',S_1,S_2)$.

• $(k'_1,k'_2)\leftarrow\mathsf{Decap}(d_{\mathrm{id}},C)$.

计算 $(\hat{k}'_1,\hat{k}'_2)\leftarrow\mathsf{Decap}'(d_{\mathrm{id}},C')$, $k'_1=\mathsf{Ext}_1(\hat{k}'_1,S_1)$ 和 $k'_2=\mathsf{Ext}_2(\hat{k}'_2,S_2)$. 输出 (k'_1,k'_2).

定理3 当 $\lambda\leqslant\min\{l'_1-l_1-\omega(\log\kappa),l'_2-l_2-\omega(\log\kappa)\}$ 时, 上述构造是泄露平滑的 T-IB-HPS.

证明 通用转换机制的正确性、通用性及有效密文与无效密文的不可区分性均可由底层的 T-IB-HPS 获得. 下面将详细证明泄露平滑性.

令 $f:\{0,1\}^*\to\{0,1\}^\lambda$ 是输出长度为 λ 的任意泄露函数. 此外, 定义一个函数 $f'(C^*,k'_1,k'_2)$, 它通过输入私钥 d_{id} 运行解封装算法 Decap 从无效封装密文 C^* 中输出相应的解封装结果 k'_1 和 k'_2, 同时输出私钥的泄露信息 $f(d_{\mathrm{id}})$, 也就是说 $f'(C^*,k'_1,k'_2)\equiv((k'_1,k'_2)\leftarrow\mathsf{Decap}(d_{\mathrm{id}},C^*),f(d_{\mathrm{id}}))$. 定义敌手的视图为 $(C^*,f(d_{\mathrm{id}}),k'_1,k'_2)$, 其中 $k'_1=\mathsf{Ext}_1(\hat{k}_1,S_1)$, $k'_2=\mathsf{Ext}_2(\hat{k}_2,S_2)$ 和 $(\hat{k}_1,\hat{k}_2)=\mathsf{Decap}'(d_{\mathrm{id}},C^*)$; 即运行解封装算法 Decap 实际是运行底层 T-IB-HPS 的解封装算法 Decap' 和强随机性提取器 Ext_1 和 Ext_2.

对于 $(\mathrm{mpk},\mathrm{msk})\leftarrow\mathsf{Setup}(1^\kappa)$ 和任意的身份 $\mathrm{id}\in\mathcal{ID}$, 有

$$\begin{aligned}
(C,f(d_{\mathrm{id}}),k'_1,k'_2)&\equiv(C,f(d_{\mathrm{id}}),k'_1=\mathsf{Ext}_1(\hat{k}_1,S_1),k'_2=\mathsf{Ext}_2(\hat{k}_2,S_2))\\
&\equiv(C^*,f'(C^*,k'_1,k'_2),k'_1=\mathsf{Ext}_1(\hat{k}_1,S_1),k'_2=\mathsf{Ext}_2(\hat{k}_2,S_2))\\
&\approx(C^*,f'(C^*,U_1,U_2),k_1=\mathsf{Ext}_1(\hat{k}_1,S_1),k_2=\mathsf{Ext}_2(\hat{k}_2,S_2))\\
&\approx(C^*,f'(C^*,U_1,U_2),\widetilde{k}_1,k_2=\mathsf{Ext}_2(\hat{k}_2,S_2))\\
&\approx(C^*,f'(C^*,U_1,U_2),\widetilde{k}_1,\widetilde{k}_2)\\
&\approx(C^*,f'(C^*,k'_1,k'_2),\widetilde{k}_1,\widetilde{k}_2)\\
&\equiv(C^*,f(d_{\mathrm{id}}),\widetilde{k}_1,\widetilde{k}_2),
\end{aligned}$$

其中 $d_{\mathrm{id}}=\mathsf{KeyGen}(\mathrm{msk},\mathrm{id})$, $C^*=\mathsf{Encap}(\mathrm{id})$, $(k'_1,k'_2)\leftarrow\mathsf{Decap}(d_{\mathrm{id}},C^*)$, $U_1\leftarrow_R\{0,1\}^{l'_1}$, $U_2\leftarrow_R\{0,1\}^{l'_2}$, $\widetilde{k}_1\leftarrow_R\{0,1\}^{l_1}$ 和 $\widetilde{k}_2\leftarrow_R\{0,1\}^{l_2}$. 此外, S_1 和 S_2 是强随机性提取器的种子.

第 1 和 4 个约等号成立是基于底层 T-IB-HPS 的平滑性; 强随机性提取器 Ext_1 和 Ext_2 的安全性保证了第 2 和 3 个约等号成立. 因此, 可得到 $\mathsf{SD}((C^*,f(d_{\mathrm{id}}),k'_1,k'_2),(C^*,f(d_{\mathrm{id}}),\widetilde{k}_1,\widetilde{k}_2))$.

由于底层的 Ext_1 和 Ext_2 分别是平均情况的 $(l'_1-\lambda,\varepsilon_1)$ 和 $(l'_2-\lambda,\varepsilon_2)$ – 强随机性提取器, 那么有

$$\lambda\leqslant l'_1-l_1-\omega(\log\kappa)\text{ 和 }\lambda\leqslant l'_2-l_2-\omega(\log\kappa).$$

综上所述, 当泄露参数满足 $\lambda \leqslant \min\{l_1' - l_1 - \omega(\log\kappa), l_2' - l_2 - \omega(\log\kappa)\}$ 时, 任意平滑的 T-IB-HPS 可借助平均情况的强随机性提取器转化为泄露平滑的 T-IB-HPS.

5 CCA 安全的抗泄露 IBE 机制的新型构造

为了设计更加高效的 CCA 安全的抗泄露 IBE 机制的通用构造, 本节将基于 T-IB-HPS 和 MAC 设计一个 CCA 安全的抗泄露 IBE 机制的新型通用构造. 此外, 由定理 3 可知, 泄露平滑的 T-IB-HPS 具备提供抗泄露攻击的能力, 因此我们采用泄露平滑的 T-IB-HPS 设计 IBE 机制的通用构造.

5.1 具体构造

令 $\Pi' = (\mathsf{Setup}', \mathsf{KeyGen}', \mathsf{Encap}', \mathsf{Encap}'^*, \mathsf{Decap}')$ 是封装密钥空间为 $\mathcal{K}_1 \times \mathcal{K}_2$, 身份空间为 $\mathcal{ID}$ 和封装密文空间为 $\mathcal{C}_1$ 的泄露平滑性 T-IB-HPS; 令 $\mathsf{MAC} = (\mathsf{Tag}, \mathsf{Ver})$ 是密钥空间 $\mathcal{K}_2$、消息空间 $\mathcal{M}$ 的消息验证码; 令 $H : \mathcal{C}_1 \times \mathcal{K}_1 \to \mathcal{M}$ 是安全的抗碰撞哈希函数. CCA 安全的抗泄露 IBE 机制的通用构造由下述算法组成:

• $(\mathrm{Params}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$.

输出 $\mathrm{Params} = (\mathrm{mpk}, \mathsf{MAC})$ 和 msk, 其中 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}'(1^\kappa)$.

• $\mathrm{sk}_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{msk}, \mathrm{id})$.

输出 $\mathrm{sk}_{\mathrm{id}} = d_{\mathrm{id}}$, 其中 $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}'(\mathrm{msk}, \mathrm{id})$.

• $C \leftarrow \mathsf{Enc}(\mathrm{id}, M)$.

计算 $(C_1, k_1, k_2) \leftarrow \mathsf{Encap}'(\mathrm{id})$, $C_2 = k_1 \oplus M$ 和 $\mathrm{Tag} \leftarrow \mathsf{Tag}(k_2, H(C_1, C_2))$. 输出 $C = (C_1, C_2, \mathrm{Tag})$.

• $M \leftarrow \mathsf{Dec}(\mathrm{sk}_{\mathrm{id}}, C)$.

计算 $(k_1', k_2') \leftarrow \mathsf{Decap}'(\mathrm{sk}_{\mathrm{id}}, C_1)$. 若有 $\mathsf{Ver}(k_2', \mathrm{Tag}, H(C_1, C_2)) = 1$ 成立, 则输出 $M = k_1' \oplus C_2$; 否则, 输出终止符 $\perp$.

5.2 安全性证明

上述通用构造的正确性可由底层泄露平滑的 T-IB-HPS 和消息验证码的正确性获得. 此外, 通用构造的抗泄露性来自底层泄露平滑的 T-IB-HPS.

定理4 若 Π' 是 λ 泄露平滑的 T-IB-HPS; MAC 是强不可伪造的消息验证码, 那么对于相应的泄露参数 λ, 上述机制是 CCA 安全的抗泄露 IBE 机制的通用构造.

证明 将通过游戏论证的方式对上述机制的 CCA 安全性进行证明, 每个游戏由模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 执行. 令事件 $\mathcal{E}_i$ 表示敌手 $\mathcal{A}$ 在游戏 Game_i 中获胜, 即有 $\Pr[\mathcal{E}_i] = \Pr[\mathcal{A} \text{ wins in } \mathsf{Game}_i]$. 特别地, 证明过程中与挑战密文相关的变量均标记为 "*", 即挑战身份和挑战密文分别是 id^* 和 $C_v^* = (C_1^*, C_2^*, \mathrm{Tag}^*)$.

令事件 $\mathcal{F}_1$ 表示敌手 $\mathcal{A}$ 在解封装询问中提交的密文 $C = (C_1, C_2, \mathrm{Tag})$ 满足条件 $(C_1, C_2) \neq (C_1^*, C_2^*)$ 和 $H(C_1, C_2) = H(C_1^*, C_2^*)$; 令事件 $\mathcal{F}_2$ 表示敌手 $\mathcal{A}$ 在获得挑战密文 $C_v^* = (C_1^*, C_2^*, \mathrm{Tag}^*)$ 之后提交了关于二元组 $(\mathrm{id}^*, (C_1^*.C_2^*, \mathrm{Tag}'))$ 的解封装询问, 其中 Tag' 是关于消息 $H(C_1^*, C_2^*)$ 的合法标签, 并且 $\mathrm{Tag}' \neq \mathrm{Tag}^*$.

Game_0: 该游戏是 IBE 机制原始泄露容忍的 CCA 安全性游戏, 其中挑战密文 $C_v^* = (C_1^*, C_2^*, \mathrm{Tag}^*)$ 的生成过程如下所述:

• 随机选取 $v \leftarrow_R \{0, 1\}$, 并计算

$$(C_1^*, k_1^*, k_2^*) \leftarrow \mathsf{Encap}'(\mathrm{id}^*),\ C_2^* = k_1^* \oplus M_v \text{ 和 } \mathrm{Tag}^* \leftarrow \mathsf{Tag}(k_2^*, H(C_1^*, C_2^*)).$$

由于该游戏是抗泄露 IBE 机制的原始 CCA 安全性游戏, 则有 $\mathsf{Adv}^{\text{LR-CCA}}_{\text{IBE},\mathcal{A}}(\kappa,\lambda)=|\Pr[\mathcal{E}_0]-\frac{1}{2}|$.

Game_1: 该游戏与 Game_0 相类似, 但该游戏在解密询问阶段增加了新的拒绝规则, 若事件 $\mathcal{F}_1$ 发生, 模拟器 $\mathcal{S}$ 拒绝敌手 $\mathcal{A}$ 提出的解密询问. 在 Game_0 中即使事件 $\mathcal{F}_1$ 发生, 模拟器 $\mathcal{S}$ 依然响应敌手 $\mathcal{A}$ 提出的解密询问; 而在 Game_1 中, 当事件 $\mathcal{F}_1$ 发生时, 模拟器 $\mathcal{S}$ 将拒绝敌手 $\mathcal{A}$ 提出的解密询问. 因此, 当事件 $\mathcal{F}_1$ 不发生时, 游戏 Game_1 和 Game_0 是不可区分的, 则有 $\Pr[\mathcal{E}_1|\overline{\mathcal{F}_1}]=\Pr[\mathcal{E}_0|\overline{\mathcal{F}_1}]$. 根据区别引理 [18] 可知 $|\Pr[\mathcal{E}_1]-\Pr[\mathcal{E}_0]|\leqslant\Pr[\mathcal{F}_1]$.

由于函数 $H:\mathcal{C}_1\times\mathcal{K}_1\to\mathcal{M}$ 是安全的抗碰撞哈希函数, 那么事件 $\mathcal{F}_1$ 发生的概率是可忽略的. 因此

$$|\Pr[\mathcal{E}_1]-\Pr[\mathcal{E}_0]|\leqslant\mathsf{negl}(\kappa).$$

Game_2: 该游戏与 Game_1 相类似, 但该游戏在解密询问阶段增加了新的拒绝规则, 即若事件 $\mathcal{F}_2$ 发生, 模拟器 $\mathcal{S}$ 拒绝敌手 $\mathcal{A}$ 提出的解密询问, 那么当事件 $\mathcal{F}_2$ 不发生时, 游戏 Game_2 和 Game_1 是不可区分的, 则有 $\Pr[\mathcal{E}_2|\overline{\mathcal{F}_2}]=\Pr[\mathcal{E}_1|\overline{\mathcal{F}_2}]$. 根据区别引理 [18] 可知 $|\Pr[\mathcal{E}_2]-\Pr[\mathcal{E}_1]|\leqslant\Pr[\mathcal{F}_2]$.

引理1 $\Pr[\mathcal{F}_2]\leqslant\mathsf{negl}(\kappa)$.

证明 假设事件 $\mathcal{F}_2$ 以压倒性的概率发生, 即敌手 $\mathcal{A}$ 获得挑战密文 $C^*_v=(C^*_1,C^*_2,\mathrm{Tag}^*)$ 之后提交了关于 $(\mathrm{id}^*,(C^*_1.C^*_2,\mathrm{Tag}'))$ 的解密询问, 其中 Tag' 是消息 $H(C^*_1,C^*_2)$ 的合法标签, 并且 $\mathrm{Tag}'\neq\mathrm{Tag}^*$.

敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 之间执行泄露容忍的 IBE 机制的 CCA 安全性游戏, 并且作为攻击者对底层消息验证码 $\mathsf{MAC}=(\mathsf{Tag},\mathsf{Ver})$ 的强不可伪造性进行攻击, 敌手 $\mathcal{B}$ 能够适应性的询问标签谕言机 $\mathsf{Tag}(k,\cdot)$ 和验证谕言机 $\mathsf{Vrify}(k,\cdot)$.

挑战阶段敌手 $\mathcal{B}$ 收到来自敌手 $\mathcal{A}$ 的挑战消息 M_0,M_1 及挑战身份 id^*, 敌手 $\mathcal{B}$ 通过下述运算生成相应的挑战密文 $C^*_v=(C^*_1,C^*_2,\mathrm{Tag}^*)$.

- 随机选取 $v\leftarrow_R\{0,1\}$, 并计算 $(C^*_1,k^*_1,k^*_2)\leftarrow\mathsf{Encap}'(\mathrm{id}^*)$ 和 $C^*_2=k^*_1\oplus M_v$.
- 发送消息 $H(C^*_1,C^*_2)$ 给标签谕言机 $\mathsf{Tag}(k,\cdot)$, 获得相应的应答 Tag^*.

敌手 $\mathcal{A}$ 获得挑战密文之后, 提交了关于二元组 $(\mathrm{id}^*,(C^*_1.C^*_2,\mathrm{Tag}'))$ 的解密询问给敌手 $\mathcal{B}$. 然后, 敌手 $\mathcal{B}$ 输出 $(\mathrm{id}^*,(C^*_1.C^*_2,\mathrm{Tag}'))$ 作为伪造的消息标签发送给挑战者. 由于 Tag' 是关于消息 $H(C^*_1,C^*_2)$ 的合法标签, 并且 $\mathrm{Tag}'\neq\mathrm{Tag}^*$, 所以敌手 $\mathcal{B}$ 输出了一个合法的消息标签对 $(H(C^*_1,C^*_2),\mathrm{Tag}')$, 攻破了底层消息验证码的强不可伪造性, 然而上述结论与底层消息验证码的安全性事实相矛盾, 因此假设不成立, 则有 $\Pr[\mathcal{F}_2]\leqslant\mathsf{negl}(\kappa)$.

由引理 1 可知 $|\Pr[\mathcal{E}_2]-\Pr[\mathcal{E}_1]|\leqslant\mathsf{negl}(\kappa)$.

Game_3: 该游戏与 Game_2 相类似, 除了挑战密文的生成阶段, 即该游戏使用挑战身份 id^* 所对应的私钥 $\mathrm{sk}_{\mathrm{id}^*}$ 计算挑战密文 $C^*_v=(C^*_1,C^*_2,\mathrm{Tag}^*)$, 具体过程描述如下:

- 计算 $\mathrm{sk}_{\mathrm{id}^*}\leftarrow\mathsf{KeyGen}(\mathrm{msk},\mathrm{id}^*)$.
- 随机选取 $v\leftarrow_R\{0,1\}$, 并计算

$(C^*_1,k^*_1,k^*_2)\leftarrow\mathsf{Encap}'(\mathrm{id}^*)$, $(\tilde{k}^*_1,\tilde{k}^*_2)\leftarrow\mathsf{Decap}'(\mathrm{sk}_{\mathrm{id}^*},C^*_1)$, $C^*_2=\tilde{k}^*_1\oplus M_v$ 和 $\mathrm{Tag}^*\leftarrow\mathsf{Tag}(\tilde{k}^*_2,H(C^*_1,C^*_2))$.

由底层泄露平滑 T-IB-HPS 机制解封装的正确性可知, 游戏 Game_3 和 Game_2 是不可区分的, 因此有 $|\Pr[\mathcal{E}_3]-\Pr[\mathcal{E}_2]|\leqslant\mathsf{negl}(\kappa)$.

Game_4: 该游戏与 Game_3 相类似, 除了挑战密文的生成阶段, 即该游戏使用无效封装算法 Encap'^* 计算挑战密文 $C^*_v=(C^*_1,C^*_2,\mathrm{Tag}^*)$, 具体过程描述如下:

- 计算 $\mathrm{sk}_{\mathrm{id}^*}\leftarrow\mathsf{KeyGen}(\mathrm{msk},\mathrm{id}^*)$.
- 随机选取 $v\leftarrow_R\{0,1\}$, 并计算

$C_1^* \leftarrow \mathsf{Encap}'^*(\mathrm{id}^*)$, $(\tilde{k}_1^*, \tilde{k}_2^*) \leftarrow \mathsf{Decap}'(\mathrm{sk}_{\mathrm{id}^*}, C_1^*)$, $C_2^* = \tilde{k}_1^* \oplus M_v$ 和 $\mathrm{Tag}^* \leftarrow \mathsf{Tag}(\tilde{k}_2^*, H(C_1^*, C_2^*))$.

由底层泄露平滑 T-IB-HPS 机制的有效封装密文与无效封装密文的不可区分性可知, 游戏 Game_4 和 Game_3 是不可区分的, 因此有 $|\Pr[\mathcal{E}_4] - \Pr[\mathcal{E}_3]| \leqslant \mathsf{negl}(\kappa)$.

Game_5: 该游戏与 Game_4 相类似, 除了挑战密文的生成阶段, 即该游戏使用从封装密钥空间 $\mathcal{K}_1 \times \mathcal{K}_2$ 中随机选取的封装密钥来计算挑战密文 $C_v^* = (C_1^*, C_2^*, \mathrm{Tag}^*)$, 具体过程描述如下:

• 随机选取 $v \leftarrow_R \{0,1\}$, 并计算

$$C_1^* \leftarrow \mathsf{Encap}'^*(\mathrm{id}^*),\ (\tilde{k}_1^*, \tilde{k}_2^*) \leftarrow_R \mathcal{K}_1 \times \mathcal{K}_2,\ C_2^* = \tilde{k}_1^* \oplus M_v \text{ 和 } \mathrm{Tag}^* \leftarrow \mathsf{Tag}(\tilde{k}_2^*, H(C_1^*, C_2^*)).$$

由底层 T-IB-HPS 机制的泄露平滑性可知, 游戏 Game_5 和 Game_4 是不可区分的, 因此有 $|\Pr[\mathcal{E}_5] - \Pr[\mathcal{E}_4]| \leqslant \mathsf{negl}(\kappa)$.

在游戏 Game_5 中, 挑战密文 $C_v^* = (C_1^*, C_2^*, \mathrm{Tag}^*)$ 已安全由随机数生成, 因此 C_v^* 中已不包含随机数 v 的任何信息, 则有 $\Pr[\mathcal{E}_5] = \frac{1}{2}$. 换句话讲, 敌手 $\mathcal{A}$ 在游戏 Game_5 中获胜的优势是可忽略的.

综上所述, 由于游戏 Game_5 和 Game_0 是不可区分的, 则敌手 $\mathcal{A}$ 在游戏 Game_0 中获胜的优势是可忽略的, 即 $|\Pr[\mathcal{E}_0] - \frac{1}{2}| \leqslant \mathsf{negl}(\kappa)$. 也就是说, 有 $\mathsf{Adv}_{\mathrm{IBE},\mathcal{A}}^{\mathrm{LR\text{-}CCA}}(\kappa, \lambda) \leqslant \mathsf{negl}(\kappa)$ 成立.

6 T-IB-HPS 的具体实例

上述 CCA 安全的抗泄露 IBE 的通用构造中, T-IB-HPS 是非常重要的底层基础工作, 本节我们将构造 T-IB-HPS 的具体实例, 并基于经典的 DBDH 假设在选择身份安全模型下对其有效封装密文与无效封装密文的不可区分性进行证明.

6.1 具体构造

• $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$.

(1) 运行群生成算法 $\mathcal{G}(1^\kappa)$ 输出相应的元组 $(p, G, g, G_T, e(\cdot))$, 其中 G 是阶为大素数 p 的循环群, g 是群 G 的生成元, $e: G \times G \to G_T$ 是高效可计算的双线性映射.

(2) 选取 3 个不同的随机数 $\alpha, \beta, \eta \leftarrow_R Z_p^*$, 并计算 $e(g,g)^\alpha$, $e(g,g)^\beta$ 和 $e(g,g)^\eta$.

(3) 随机选取 $u, h \leftarrow_R G$, 公开系统参数 mpk, 同时秘密保存主密钥 msk, 其中

$$\mathrm{mpk} = (g, u, h, e(g,g)^\alpha, e(g,g)^\beta, e(g,g)^\eta) \text{ 和 } \mathrm{msk} = (g^\alpha, g^\beta, g^\eta).$$

• $d_{\mathrm{id}} \leftarrow \mathsf{KeyGen}(\mathrm{id}, \mathrm{msk})$.

(1) 随机选取 $r, t \leftarrow_R Z_p^*$, 计算 $d_1 = g^\alpha g^{-\eta t}(u^{\mathrm{id}}h)^r$, $d_2 = g^\beta g^{-\eta t}(u^{\mathrm{id}}h)^r$, $d_3 = g^{-r}$ 和 $d_4 = t$.

(2) 输出身份 id 所对应的私钥 $d_{\mathrm{id}} = (d_1, d_2, d_3, d_4)$.

• $(C, k_1, k_2) \leftarrow \mathsf{Encap}(\mathrm{id})$.

(1) 随机选取 $z \leftarrow_R Z_p^*$, 计算 $c_1 = g^z$, $c_2 = (u^{\mathrm{id}}h)^z$ 和 $c_3 = e(g,g)^{\eta z}$.

(2) 计算 $k_1 = e(g,g)^{\alpha z}$ 和 $k_2 = e(g,g)^{\beta z}$.

(3) 输出有效封装密文 $C = (c_1, c_2, c_3)$ 及相对应的封装密钥对 (k_1, k_2).

• $C^* \leftarrow \mathsf{Encap}^*(\mathrm{id})$.

(1) 随机选取 $z, z' \leftarrow_R Z_p^*$ 且 $z \neq z'$, 计算 $c_1 = g^z$, $c_2 = (u^{\mathrm{id}}h)^z$ 和 $c_3 = e(g,g)^{\eta z'}$.

(2) 输出无效封装密文 $C^* = (c_1, c_2, c_3)$.

• $(k_1', k_2') \leftarrow \mathsf{Decap}(d_{\mathrm{id}}, C)$.

(1) 计算 $k_1' = e(c_1, d_1)e(c_2, d_3)c_3^{d_4}$ 和 $k_2' = e(c_1, d_2)e(c_2, d_3)c_3^{d_4}$.

(2) 输出相应的解封装结果 (k_1', k_2').

6.2 安全性分析

6.2.1 正确性

由下述等式即可获得本文上述 T-IB-HPS 实例的正确性.

$$k_1' = e(c_1, d_1)e(c_2, d_3)c_3^{d_4} = e(g^z, g^{\alpha}g^{-\eta t}(u^{\mathrm{id}}h)^r)e((u^{\mathrm{id}}h)^z, g^{-r})e(g,g)^{\eta zt} = e(g,g)^{\alpha z};$$

$$k_2' = e(c_1, d_2)e(c_2, d_3)c_3^{d_4} = e(g^z, g^{\beta}g^{-\eta t}(u^{\mathrm{id}}h)^r)e((u^{\mathrm{id}}h)^z, g^{-r})e(g,g)^{\eta zt} = e(g,g)^{\beta z}.$$

特别地, 由 $\alpha \neq \beta$ 可知 $k_1' \neq k_2'$, 并且由 α 和 β 的随机性确保了 k_1' 和 k_2' 对任意敌手而言是完全随机的.

6.2.2 通用性

对于身份 id 的私钥 $d_{\mathrm{id}} = (d_1, d_2, d_3, d_4)$ 及相应的无效封装算法 Encap^* 输出的无效封装密文 $C^* = (c_1, c_2, c_3)$, 由解封装算法可知 $k_1' = e(g,g)^{\alpha z}e(g,g)^{\eta t(z'-z)}$ 和 $k_2' = e(g,g)^{\beta z}e(g,g)^{\eta t(z'-z)}$. 由此可见, 无效封装密文 C^* 的解封装结果中包含了相应私钥 d_{id} 的底层随机数 t. 由于同一个身份 id 的不同私钥 d_{id} 和 d_{id}' 是由不同的底层随机数 t 和 t' 生成, 因此, 对于任意的敌手而言, 同一身份 id 的不同私钥 d_{id} 和 d_{id}' 对同一无效密文 $C^* = (c_1, c_2, c_3)$ 的解封装视图是各不相同的, 因此有 $\Pr[\mathsf{Decap}(C^*, d_{\mathrm{id}}) = \mathsf{Decap}(C^*, d_{\mathrm{id}}')] \leqslant \mathsf{negl}(\kappa)$ 成立. 换句话讲, 在 T-IB-HPS 中, 不同的身份私钥对相应无效封装密文的解封装结果是各不相同的.

6.2.3 平滑性

对于身份 id 的私钥 $d_{\mathrm{id}} = (d_1, d_2, d_3, d_4)$ 及相应的无效封装算法 Encap^* 输出的无效封装密文 $C^* = (c_1, c_2, c_3)$, 由通用性可知 $k_1' = e(g,g)^{\alpha z}e(g,g)^{\eta t(z'-z)}$ 和 $k_2' = e(g,g)^{\beta z}e(g,g)^{\eta t(z'-z)}$. 对于任意的敌手而言, 参数 α, β, η, t, z 和 z' 都是从 Z_p^* 中均匀随机选取的; 换句话讲, 在敌手看来 k_1' 和 k_2' 都是均匀随机的, 因此有 $\mathsf{SD}((C^*, k_1', k_2'), (C^*, \hat{k}_1, \hat{k}_2))$ 成立, 其中 $\hat{k}_1 \leftarrow_R G_T$ 和 $\hat{k}_2 \leftarrow_R G_T$. 换句话讲, 在 T-IB-HPS 中, 对于任意的无效封装密文, 解封装算法将输出封装密钥空间上的两个随机值.

6.2.4 有效封装密文与无效封装密文的不可区分性

定理5 在选择身份安全模型下, 若存在一个 PPT 敌手 $\mathcal{A}$ 在多项式时间内能以不可忽略的优势区分有效封装密文与无效封装密文, 那么我们就能够构造一个敌手 $\mathcal{B}$ 在多项式时间内能以显而易见的优势攻破经典的 DBDH 困难性假设.

证明 假设敌手 $\mathcal{A}$ 能以优势 $\mathsf{Adv}^{\text{VI-IND}}_{\text{T-IB-HPS},\mathcal{A}}(\kappa)$ 区分本文 T-IB-HPS 实例的效封装密文与无效封装密文. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 开始有效封装密文与无效封装密文区分性游戏之前, 敌手 $\mathcal{B}$ 从 DBDH 假设的挑战者处获得一个 DBDH 挑战元组 $(g, g^{\alpha}, g^{\beta}, g^{c}, T_{\omega})$ 及相应的公开元组 $(p, G, g, G_T, e(\cdot))$, 其中 $a, b, c, c' \leftarrow_R Z_p^*$, $T_1 = e(g,g)^{abc}$ 和 $T_0 = e(g,g)^{abc'}$. 根据选择身份安全模型的要求, 在游戏开始之前, 敌手 $\mathcal{A}$ 将选定的挑战身份 id^* 发送给敌手 $\mathcal{B}$. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间的消息交互过程具体如下所示:

• **初始化.** 该阶段敌手 $\mathcal{B}$ 执行下述操作:

(1) 令 $u = g^a$, 随机选取 $y \leftarrow_R Z_p^*$, 计算 $h = (g^a)^{-\mathrm{id}^*}g^y$.

(2) 随机选取 $\alpha', \beta', t^* \leftarrow_R Z_p^*$, 计算

$$e(g,g)^{\eta}=e(g^a,g^b),\ e(g,g)^{\alpha}=e(g^a,g^b)^{t^*}e(g,g)^{\alpha'}\ \text{和}\ e(g,g)^{\beta}=e(g^a,g^b)^{t^*}e(g,g)^{\beta'}.$$

特别地, 通过上述运算敌手 $\mathcal{B}$ 隐含地设置了 $\eta=ab$, $\alpha=\eta t^*+\alpha'$ 和 $\beta=\eta t^*+\beta'$.

(3) 发送公开参数 $\mathrm{mpk}=(g,u,h,e(g,g)^{\alpha},e(g,g)^{\beta},e(g,g)^{\eta})$ 给敌手 $\mathcal{A}$.

注意到 α', β' 和 t^* 是由敌手 $\mathcal{A}$ 从 Z_p^* 中均匀随机选取, a 和 b 由 DBDH 挑战者从 Z_p^* 中均匀随机选取. 因此, 对于敌手 $\mathcal{A}$ 而言, mpk 中的公开参数都是均匀随机的, 即模拟游戏与真实环境是不可区分的.

• **阶段 1.** 敌手 $\mathcal{A}$ 能够适应性的对身份空间 $\mathcal{ID}$ 中的任意身份 $\mathrm{id}\in\mathcal{ID}$ 进行密钥生成询问 (包括挑战身份 id^*), 敌手 $\mathcal{B}$ 分下述两类情况处理敌手 $\mathcal{A}$ 关于身份 id 的密钥生成询问:

(1) $\mathrm{id}\neq\mathrm{id}^*$. 敌手 $\mathcal{B}$ 随机选取 $r',t'\leftarrow_R Z_p^*$, 输出身份 id 所对应的私钥

$$d_{\mathrm{id}}=(d_1,d_2,d_3,d_4)=(g^{\alpha'}(g^b)^{-\frac{yt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'},g^{\beta'}(g^b)^{-\frac{yt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'},g^{-r'}(g^b)^{\frac{t'}{\mathrm{id}-\mathrm{id}^*}},t^*-t').$$

对于随机选取的 $r',t'\leftarrow_R Z_p^*$, 存在随机数 $r,t\in Z_p^*$, 满足 $r=r'-\frac{bt'}{\mathrm{id}-\mathrm{id}^*}$ 和 $t=t^*-t'$, 则有

$$\begin{aligned}
g^{\alpha'}(g^b)^{-\frac{yt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}&=g^{abt^*+\alpha'}(g^{-abt^*+abt'})g^{-abt'}(g^b)^{\frac{-yt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}\\
&=g^{\alpha}(g^{-abt^*+abt'})g^{-abt'}(g^y)^{\frac{-bt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}\\
&=g^{\alpha}(g^{ab})^{-(t^*-t')}(g^{a(\mathrm{id}-\mathrm{id}^*)}g^y)^{\frac{-bt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}\\
&=g^{\alpha}(g^{ab})^{-(t^*-t')}(u^{\mathrm{id}}h)^{\frac{-bt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}\\
&=g^{\alpha}g^{-\eta(t^*-t')}(u^{\mathrm{id}}h)^{r'-\frac{bt'}{\mathrm{id}-\mathrm{id}^*}}\\
&=g^{\alpha}g^{-\eta t}(u^{\mathrm{id}}h)^{r},\\
g^{\beta'}(g^b)^{-\frac{yt'}{\mathrm{id}-\mathrm{id}^*}}(u^{\mathrm{id}}h)^{r'}&=g^{\beta}g^{-\eta t}(u^{\mathrm{id}}h)^{r},\\
g^{-r'}(g^b)^{\frac{t'}{\mathrm{id}-\mathrm{id}^*}}&=g^{-(r'-\frac{bt'}{\mathrm{id}-\mathrm{id}^*})}=g^{-r}.
\end{aligned}$$

因此, 敌手 $\mathcal{B}$ 输出了身份 id 对应的有效私钥 d_{id}.

(2) $\mathrm{id}=\mathrm{id}^*$. 敌手 $\mathcal{B}$ 随机选取 $r^*\leftarrow_R Z_q^*$, 输出身份 id 相对应的私钥

$$d_{\mathrm{id}}=(d_1,d_2,d_3,d_4)=(g^{\alpha'}(u^{\mathrm{id}}h)^{r^*},g^{\beta'}(u^{\mathrm{id}}h)^{r^*},g^{-r^*},t^*).$$

由于 $g^{\alpha'}(u^{\mathrm{id}}h)^{r^*}=g^{\alpha-\eta t^*}(u^{\mathrm{id}}h)^{r^*}=g^{\alpha}g^{-\eta t^*}(u^{\mathrm{id}}h)^{r^*}$ 和 $g^{\beta'}(u^{\mathrm{id}}h)^{r^*}=g^{\beta-\eta t^*}(u^{\mathrm{id}}h)^{r^*}=g^{\beta}g^{-\eta t^*}(u^{\mathrm{id}}h)^{r^*}$, 因此敌手 $\mathcal{B}$ 输出了挑战身份 id^* 对应的有效私钥 d_{id^*}.

• **挑战.** 敌手 $\mathcal{B}$ 首先计算 $c_1=g^c$, $c_2=(g^c)^y$ 和 $c_3=T_{\omega}$, 然后输出挑战密文 $C_v^*=(c_1,c_2,c_3)$ 给敌手 $\mathcal{A}$, 其中 $(u^{\mathrm{id}^*}h)^c=(g^{a\mathrm{id}^*}(g^a)^{-\mathrm{id}^*}g^y)=(g^c)^y$.

• **阶段 2.** 与阶段 1 相类似, 敌手 $\mathcal{A}$ 能够适应性的对任意身份 $\mathrm{id}\in\mathcal{ID}$ 进行密钥生成询问 (包括挑战身份 id^*), 敌手 $\mathcal{B}$ 按与阶段 1 相同的方式返回相应的应答 d_{id}.

• **输出.** 敌手 $\mathcal{A}$ 输出对 v 的猜测 v'. 若 $v'=v$, 则敌手 $\mathcal{B}$ 输出 $\omega=1$, 意味着 $\mathcal{B}$ 能够解决 DBDH 假设; 否则, 敌手 $\mathcal{B}$ 输出 $\omega=0$.

分下述两类情况讨论挑战密文 $C_v^*=(c_1,c_2,c_3)$:

(1) $T_{\omega}=e(g,g)^{abc}$. 有 $c_3=e(g,g)^{abc}=e(g,g)^{\eta c}$, 此时挑战密文 $C_v^*=(c_1,c_2,c_3)$ 是关于挑战身份 id^* 的有效封装密文.

(2) $T_\omega = e(g,g)^{abc'}$ 且 $c' \neq c$. 有 $c_3 = e(g,g)^{abc} = e(g,g)^{\eta c'}$, 此时挑战密文 $C_v^* = (c_1, c_2, c_3)$ 是关于挑战身份 id^* 的无效封装密文.

综上所述, 如果敌手 $\mathcal{A}$ 能以不可忽略的优势 $\mathsf{Adv}^{\text{VI-IND}}_{\text{T-IB-HPS},\mathcal{A}}(\kappa)$ 区分有效封装密文与无效封装密文, 且 $\mathcal{B}$ 将 $\mathcal{A}$ 以子程序的形式运行, 那么敌手 $\mathcal{B}$ 能以显而易见优势 $\mathsf{Adv}^{\text{DBDH}}_{\mathcal{B}} \geqslant \mathsf{Adv}^{\text{VI-IND}}_{\text{T-IB-HPS},\mathcal{A}}(\kappa)$ 攻破经典的 DBDH 困难性假设.

7 结论

本文为构造更加高效的 CCA 安全的抗泄露 IBE 机制的通用构造, 首先提出了一个新的密码学原语, 称其为双封装密钥的身份基哈希证明系统; 然后, 基于双封装密钥的身份基哈希证明系统和带密钥的消息验证码提出了 CCA 安全的抗泄露 IBE 机制的新型通用构造, 我们的构造中并未使用 NIZK, OT-LF 和 OTS 等计算效率低的密码学基础原语, 并且相应通用构造的抗泄露性能完全由底层的泄露平滑的 T-IB-HPS 决定; 最后, 为了展示本文通用结构的可用性, 我们设计了 T-IB-HPS 的具体实例, 并基于 DBDH 假设对实例的安全性进行了形式化证明. 综上所述, 本文提出了实用的构造高效 CCA 安全的抗泄露 IBE 机制的新方法.

下一阶段, 在可更新 IB-HPS 的研究基础上, 继续研究可更新 T-IB-HPS 的实例化, 推进对连续泄露容忍的 CCA 安全的 IBE 机制高效通用构造方法的研究. 此外, 在公钥环境下, 文献 [19] 提出了通过任意 PKE 机制构造 HPS 的通用方法, 下一阶段非常有必要在该技术的基础上研究通过其他密码机制设计 T-IB-HPS 的通用构造, 以达到基于静态安全性假设设计适应性安全的 T-IB-HPS 实例的目的.

参考文献

1 Naor M, Segev G. Public-key cryptosystems resilient to key leakage. In: Proceedings of the 29th Annual International Cryptology Conference, Santa Barbara, 2009. 18–35

2 Qin B D, Liu S L. Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 381–400

3 Qin B D, Liu S L. Leakage-flexible CCA-secure public-key encryption: simple construction and free of pairing. In: Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, 2014. 19–36

4 Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, 2004. 207–222

5 Boneh D, Katz J. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In: Proceedings of Cryptographers' Track at the RSA Conference, San Francisco, 2005. 87–103

6 Dodis Y, Haralambiev K, López-Alt A, et al. Cryptography against continuous memory attacks. In: Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science, Las Vegas, 2010. 511–520

7 Alwen J, Dodis Y, Naor M, et al. Public-key encryption in the bounded-retrieval model. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco, 2010. 113–134

8 Zhou Y W, Yang B, Mu Y. The generic construction of continuous leakage-resilient identity-based cryptosystems. Theor Comput Sci, 2019, 772: 1–45

9 Zhou Y W, Yang B, Xia Z, et al. Anonymous and updatable identity-based hash proof system. IEEE Syst J, 2019, 13: 2818–2829

10 Zhou Y W, Yang B, Wang T, et al. Novel updatable identity-based hash proof system and its applications. Theor Comput Sci, 2020, 804: 1–28

11 Zhou Y W, Yang B, Xia Z, et al. Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. Theor Comput Sci, 2020, 809: 277–295
12 Nishimaki R, Yamakawa T. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio. In: Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, 2019. 466–495
13 Yuen T H, Chow S S M, Zhang Y, et al. Identity-based encryption resilient to continual auxiliary leakage. In: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 117–134
14 Zhou Y W, Yang B, Mu Y. Continuous leakage-resilient identity-based encryption with leakage amplification. Des Codes Cryptogr, 2019, 87: 2061–2090
15 Dodis Y, Haralambiev K, López-Alt A, et al. Efficient public-key cryptography in the presence of key leakage. In: Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010. 613–631
16 Alwen J, Dodis Y, Naor M, et al. Public-key encryption in the bounded-retrieval model. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco, 2010. 113–134
17 Zhou Y W, Yang B. Continuous leakage-resilient public-key encryption scheme with CCA security. Comput J, 2017, 60: 1161–1172
18 Liu S L, Weng J, Zhao Y L. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks. In: Proceedings of Cryptographers' Track at the RSA Conference, San Francisco, 2013. 84–100
19 Hazay C, López-Alt A, Wee H, et al. Leakage-resilient cryptography from minimal assumptions. In: Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, 2013. 160–176

A new construction of leakage-resilient CCA secure IBE scheme

Yanwei ZHOU[1,2,3], Bo YANG[1*], Zhe XIA[4] & Mingwu ZHANG[2,3]

1. *School of Computer Science, Shaanxi Normal University, Xi'an* 710062*, China*;
2. *State Key Laboratory of Cryptology, Beijing* 100878*, China*;
3. *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin* 541004*, China*;
4. *School of Computer Science and Technology, Wuhan University of Technology, Wuhan* 430070*, China*
* Corresponding author. E-mail: byang@snnu.edu.cn

Abstract Leakage of private information has become a threat to the security of cryptography systems. It has become a common security requirement that a cryptography scheme should withstand various leakage attacks. The non-interactive zero-knowledge (NIZK) argument system, one-time lossy filter (OT-LF) and one-time signature were widely used to create the generic constructions of leakage-resilient identity-based encryption (IBE) scheme with chosen-ciphertext attack (CCA) security. However, the computational efficiency of the corresponding generic construction is low because the underlying cryptographic tool is low. Thus, to solve the above problem, a new cryptographic primitive, called identity-based hash proof system with two encapsulated-key (T-IB-HPS), is proposed. The new generic constructions of leakage resilient IBE scheme with CCA security is created from the T-IB-HPS and message authentication code (MAC), and the security of the above proposed scheme is proved from the security of the underlying cryptographic tool. To further show the practicability, an instantiation of T-IB-HPS is constructed, and the formal security proof of the above instantiation is shown based on the decisional bilinear Diffie-Hellman (DBDH) assumption. Compared with the previous generic constructions of leakage resilient IBE scheme with CCA security, since the underlying cryptographic tools with low computational efficiency are not used, our generic construction has high computational efficiency.

Keywords Hash proof system, identity-based Hash proof system, identity-based encryption, leakage resilience

Yanwei ZHOU was born in 1986, and received his Ph.D. degree in computer software and theory from the Shaanxi Normal University, in 2018. He is currently a senior engineer with the School of Computer Science, Shaanxi Normal University, China. His research interests include leakage-resilient cryptography and anonymous communication.

Zhe XIA was born in 1982, and received his Ph.D. degree from the University of Surrey, in 2009. He is currently an associate professor with the Department of Computer Science, Wuhan University of Technology, China. He serves as the associate editor for the Journal of Information Security Applications. His research interests include secure e-voting protocols, secret sharing, and secure multiparty computation.

Bo YANG was born in 1963, and received his Ph.D. degree in cryptography from the Xidian University, in 1999. He has been currently a professor at the School of Computer Science at the Shaanxi Normal University. His research interests include information security and cryptography.

Mingwu ZHANG was born in 1970, and received his Ph.D. degree from the South China Agricultural University, in 2009. He has been currently a professor in the School of Computer Science and Information Security at the Guilin University of Electronic Technology, China. His research interests include cryptography technology for network and data security, secure computation, privacy preservation.