

基于不同监管策略下的身份基变形加密方案

赵一, 李思琦, 明洋, 张启福
(长安大学信息工程学院, 陕西 西安 710121)

摘要: 现代传统加密方案建立在用户私钥保密、用户可自主控制通信消息两大安全前提之上, 若监管方掌握用户私钥, 用户隐私通信安全就会受到挑战, 变形加密的提出, 可在此场景下实现安全隐蔽通信, 随着身份基加密的广泛应用, 身份基变形加密成为新的研究热点。本文面向两类监管机制, 设计具备访问控制能力的身份基变形加密通道。针对监管约束较弱、允许采用身份基加密的场景, 依托同类方案结构自相似性搭建同构变形框架, 借助密文随机分量实现隐蔽信息提取, 兼顾密文外观一致性与方案可迁移性, 并完成经典方案实例化。面向仅允许公钥加密的强约束场景, 构建双层异构变形框架, 表层承载常规通信, 底层内嵌身份基机制实现访问权限管控, 结合具体加密算法保证密文形态合规, 同时设计双密钥解耦机制, 即便常规私钥泄露, 仍可保障隐蔽通信安全。

关键词: 变形加密; 公钥加密; 无证书公钥加密; 身份基加密; 身份基变形加密

中图分类号: TP309

文献标志码: A

doi:xxxx

Identity Based Anamorphic Encryption under Various Regulatory Strategies

Zhao Yi, Li Siqi, Ming Yang, Zhang Qifu

School of Information Engineering, Chang'an University, Xi'an 710121, China

Abstract: Modern traditional encryption relies on two premises: user autonomy in message selection and private key confidentiality. When regulators obtain private keys, privacy communication is threatened. Anamorphic encryption enables secure covert communication, and identity based anamorphic encryption has become a research focus with the wide use of identity based encryption. This paper designs identity based anamorphic encryption channels with access control for two regulatory scenarios. For weakly regulated settings allowing identity based encryption, a homogeneous framework leverages structural similarity to achieve covert extraction via ciphertext randomness, balancing consistency and transferability. For highly constrained scenarios only permitting public key encryption, a dual-layer heterogeneous framework ensures compliance and security even if regular keys are leaked.

Key words: Anamorphic encryption, Public key encryption, Certificateless public key encryption, Identity based encryption, Identity based anamorphic encryption

收稿日期: XXXX-XX-XX; 修回日期: XXXX-XX-XX

通信作者: 赵一, yizhao@chd.edu.cn

基金项目: 国家自然科学基金资助项目 (No. 62472049, No. 62602070); 陕西省自然科学基金资助项目 (No. 2025JC-YBMS-741); 陕西省重点研发计划基金资助项目 (No. 2024GX-YBXM-078)

Foundation Items: The National Natural Science Foundation of China (No. 62472049, No. 62602070), The Natural Science Basic Research Program of Shaanxi (No. 2025JC-YBMS-741), The Key Research and Development Program of Shaanxi Province (No. 2024GX-YBXM-078)

0 引言

在密码学的发展历史中,学术界致力于寻找信息隐私保护与系统合规管理之间的平衡。现代传统加密方案建立在两个前置假设之上:其一是发送者自由假设,即在宽松数据交互环境中,发送方可自由选择通信内容;其二是接收者隐私假设,即接收方可独立保管私钥,外部实体无法越权获取^[1]。然而近年来,斯诺登事件披露,部分强力机构可通过大规模监控与密钥介入等方式,直接打破上述两项核心安全假设。关于密码技术的应用边界引发了旷日持久的学术探讨与行业争议,这种现象在早期产生了不同技术理念的深度碰撞。

面对受限审计环境,后门攻击^[2-5]、窃密术^[6-7]、隐写术^[8]与合规需求深度冲突,学术界开始探索在合法算法里搭建隐蔽信道。2022年,变形加密(Anamorphic Encryption, AME)^[1]被正式提出,它不再试图在既有协议的漏洞中寻找生存空间,而是重新构筑了透明环境下的通信法则。AME的核心精髓在于同一串密文能够在不同的观测维度下展现出截然不同的信息形态。在常规的审查视角中,这仅是一段符合监管规范的普通消息。但对于掌握了特殊代数关系或内部共享参数的通信参与者而言,这层合规的密文外壳便化作了绝佳的数据隐蔽载体,用户严格遵守规范、使用指定算法、配合密钥托管,只利用加密随机性,在合法密文中藏一条秘密通道。既不与审查机制冲突,又能实现隐蔽通信。

身份基加密(Identity based Encryption, IBE)^[9-10]现已在大规模系统中得到广泛应用,其密钥管理的方式简洁高效,基于此,学术界敏锐地洞察到变形范式与IBE之间存在着天然的逻辑契合点。身份基加密凭借其独特的集中式密钥生成机制,能够将复杂的公钥基础设施简化为直观的身份标识,这不仅极大地优化了管理流程,也为监管方构建可控、可预测的通信系统提供了选择,随着应用场景的演进,AME逐渐扩展至身份基变形加密(Identity based Anamorphic Encryption, IBAE)^[11]这样更具表达力的领域。

然而,深入剖析现有的身份基变形加密研究,系统在面对复杂多变的情况时仍面临三大现实痛点:

1. 结构高度绑定与可迁移性缺失的矛盾:现有

IBAE构造与其具体的底层算法流程深度绑定,缺乏通用转化框架。一旦底层IBE方案因安全假设更新或性能升级而需要替换,既有的变形信道将直接失效,导致方案难以在不同密码学体系中迁移与标准扩展。

2. 密钥集中托管与常规私钥泄露的隐蔽失效风险:变形用户组模型高度依赖地下集中托管的主私钥,且解密时往往需同时依赖常规私钥与变形密钥。一旦管理者节点受损或接收者的常规私钥被监管方审查获取,整个隐蔽通信防线将面临单点崩溃与行为暴露风险。

3. 监管机制更迭与细粒度访问控制缺失的矛盾:当行业标准或监管制度收紧,强约束监管方强制限定只能运行标准公钥加密(Public key encryption, PKE)并禁止直接执行IBE时,传统基于IBE的变形通道将因数学结构不兼容而直接失效,导致变形用户组失去细粒度的身份访问控制能力。

为了打破上述困局,本文面向两类不同的监管机制,系统性地构建并实现了具备访问控制能力的身份基变形加密通道:

1. 同构方案(面向允许IBE的监管场景):解决已有方案结构碎片化与难以迁移的问题。通过抽样与自相似性将隐蔽通道建立于同类原语叠加之上,在保持密文同构的同时实现了非对称与鲁棒的隐蔽通信。

2. 异构方案(面向仅允许PKE的监管场景):采用双层架构,表层承载标准PKE通信、底层嵌入IBE逻辑。本文引入双密钥解耦设计,隔离常规密钥与变形密钥的功能,避免隐蔽行为暴露;同时采用去中心化密钥生成机制,分散管理者权限、消除单点故障风险,有效解决监管收紧后变形通道失效与访问控制。

1 相关工作

Persiano等学者^[1]在早期研究中确立了AME的理论框架,一类是发送者变形加密^[1,12-13],一类是接收者变形加密^[14-19],本文主要探讨接收者变形加密(以下简称变形加密)。核心概念是提出通信双方可以预先共享双密钥(double key, dkey)。接收方利用dkey就能从看似普通的密文中提取出额外内容,隐蔽信道多局限于点对点通信^[1,12,15],一方暴露即可能导致信道泄露。为了突破这一局限,后

期研究提出影子接收者^[14,16]概念,允许发送方在向表面接收者传递表层消息的同时,将隐蔽消息定向投递给网络中未被公开标识的影子接收者。随后,AME 还演化出了公钥变形加密^[20]、变形签名^[18,21-22]、变形认证密钥交换^[17]、广播变形加密^[23]等概念。

随着 AME 向 IBAE 领域延伸,变形用户组的概念应运而生。在这种架构中,通常由一个地下的可信管理者进行集中管理。管理者利用系统的底层主私钥,为变形成员分发与身份绑定的底层身份密钥。社群成员在表面上完全遵循监管方标准加密规范开展常规通信,但在暗中,他们凭借底层密钥通过合规密文传递秘密指令,形成了一套平行于公开网络的隐蔽通信秩序。Banerjee 等学者^[11]在 AME 向 IBAE 加密演进的过程中起到了至关重要的桥梁作用。其提出的理论框架和技术手段直接为 IBAE 加密的实现提供了底层支撑,通过多消息扩展和无需预共享密钥的公钥变形加密模型,为 IBAE 加密扫清了技术障碍。

2 预备知识

本节介绍构建方案时用到的密码学原语。首先给出变形加密的定义,随后引入用于弱监管同构方案的 BB04 身份基加密,以及用于强监管异构方案的无配对无证书加密,最后定义安全性需求与代数困难假设。

2.1 变形加密

设 $\Pi = (KG, Enc, Dec)$ 为标准 PKE 方案,基于 Π 构造的 AME 方案 $\sum = (aKG, aEnc, aDec)$ 由以下算法组成:

变形密钥生成算法 $aKG(1^\lambda)$: 输入安全参数 λ , 输出 $(apk, ask, dkey)$ 。其中变形公私钥 (apk, ask) 的分布应与标准 PKE 方案 KG 算法生成的公私钥 (pk, sk) 在计算上不可区分, $dkey$ 为双密钥。

变形加密算法 $aEnc(dkey, apk, msg, amsg)$: 输入变形公钥 apk 、双密钥 $dkey$ 、常规消息 msg 以及隐蔽变形消息 $amsg$, 输出变形密文 c 。

变形解密算法 $aDec(dkey, c)$: 输入双密钥 $dkey$ 和变形密文 c , 输出变形消息 $amsg$ 。

2.2 Boneh-Boyen 身份基加密方案

Boneh-Boyen 身份基加密方案是由 Boneh 和 Boyen 学者^[10]在 2004 年提出的 (以下简称为 BB04

方案)。

初始化算法。系统输入基础群参数,从群 G_1 中随机选择生成元 (u, g, h) , 并从 $\mathbb{Z}_p^*$ 群中随机选择主密钥 a , 计算映射函数 $F(x) = u^x h$, 计算双线性对 $e(g, g)^a$, 输出主密钥 $msk = a$, 公开系统参数 $P_{pub} = \{u, g, h, e(g, g)^a\}$ 。

密钥提取算法。密钥生成中心输入接收者的身份标识 id 与主密钥 a , 从 $\mathbb{Z}_p^*$ 群随机选择盲化因子 r , 计算私钥组件 $d_1 = g^a (F(id))^r$ 和 $d_2 = g^r$, 输出用户私钥 (d_1, d_2) 。

加密算法。发送方输入接收者身份 id 、明文消息 M 与公开参数 P_{pub} , 从 $\mathbb{Z}_p^*$ 群随机选择加密因子 s , 计算密文组件 $C_1 = Me(g, g)^{as}$ 、 $C_2 = g^s$ 与 $C_3 = (F(id))^s$, 输出完整密文 $C = (C_1, C_2, C_3)$ 。

解密算法: 接收方输入收到的密文 C 与自身的私钥 (d_1, d_2) , 计算双线性对公式 $C_1 \cdot \frac{e(d_2, C_3)}{e(d_1, C_2)}$, 输出恢复的原始明文消息 M 。

2.3 无配对无证书公钥加密系统

无配对无证书公钥加密方案 (Certificateless Public Key Encryption without Pairing, CLPKE) 由 Baek 等学者^[24]在 2005 年提出, 具体算法如下:

初始化算法。密钥生成中心生成两个大素数 p 和 q , 满足 q 能够整除 $p - 1$ 的条件。在乘法群 $\mathbb{Z}_p^*$ 中选取一个生成元 g , 随机选取一个系统主私钥 $x \in \mathbb{Z}_q^*$, 并且计算出主公钥 $y = g^x$, 选择三个哈希函数 H_1 、 H_2 和 H_3 。最后, 密钥生成中心公开发布系统公共参数 $params = (p, q, g, y = g^x, H_1, H_2, H_3)$, 同时保密主密钥 $masterkey = x$ 。

部分密钥提取算法。密钥生成中心输入用户的身份标识符 id , 随机选取一个数值 $s \in \mathbb{Z}_q^*$, 利用该数值计算出部分公钥 $w = g^s$ 。接着, 计算出部分私钥 $t = s + xH_1(id, w)$ 。将部分密钥对 $(P_{id}, D_{id}) = (w, t)$ 发送给用户。

秘密值设置算法。用户随机选择一个数值 z , 将数值 z 设置为自己的秘密值 s_{id} 。

私钥设置算法。用户组合秘密值 z 和部分私钥 t , 生成最终的完整的用户私钥 $SK_{id} = (z, t)$ 。

公钥设置算法。用户输入秘密值 s_{id} 和部分公钥 P_{id} , 计算 $\eta = g^{s_{id}}$, 生成完整的用户公钥 $PK_{id} = (w, \eta)$ 。

加密算法。发送方取得接收方的身份标识符 id 和公钥 PK_{id} , 输入明文 M , 计算 $\gamma_{id} = w\gamma^{H_1(id,w)}$, 随机挑选一个比特串 σ , 计算随机数 $r = H_2(M, \sigma)$, 计算两个会话密钥 $k_1 = \eta^r$ 和 $k_2 = \gamma_{id}^r$, $c_1 = g^r$ 为密文的第一部分, $c_2 = H_3(k_1, k_2) \oplus (M || \sigma)$ 为密文的第二部分, 输出最终密文 $C = (c_1, c_2)$ 。

解密算法。接收方输入完整私钥 SK_{id} , 提取私钥 SK_{id} 得到 z 和 t , 计算 $H_3(c_1^z, c_2^t) \oplus c_2$, 通过计算结果得到明文 M 和 σ , 检查等式 $g^{H_2(M, \sigma)} = c_1$, 等式成立则输出明文 M 。

2.4 安全性需求

表1 真实游戏

真实游戏 $RealG_A(\lambda)$
1. 密钥生成算法 KG 生成公私钥 (pk, sk)
2. 调用加密谕言机 EO , 返回 $A^{EO(pk, \cdot)}(pk, sk)$, 具体流程如下:
$EO(pk, msg, amsg) = ct$ $msg = (msg_1, msg_2), ct = (ct_1, ct_2)$ $ct_i = Enc(pk, msg_i), i = \{1, 2\}$

定义 2.1 变形安全性: 设 $\Sigma = (aKG, aEnc, aDec)$ 为基于方案 $\Pi = (KG, Enc, Dec)$ 的变形加密方案。若对任意多项式时间敌手 $\mathcal{A}$, 表1和表2中定义的安全游戏满足以下条件, 则称方案 Σ 满足变形安全性:

$$|Pr[RealG_A(\lambda) = 1] - Pr[AnamG_A(\lambda) = 1]| \leq \text{negl}(\lambda)$$

表2 变形游戏

变形游戏 $AnamG_A(\lambda)$
1. 密钥生成算法 aKG 生成密钥对 $((apk, ask), (dpk, dsk))$
2. 调用变形加密谕言机 aO , 返回 $A^{aO(apk, dpk, \cdot)}(apk, ask)$, 具体流程如下:
$aO(apk, dpk, msg, amsg) = ct$ $msg = (msg_1, msg_2), ct = (ct_1, ct_2)$ $ct = aEnc(apk, dpk, msg, amsg)$

定义 2.2 选择明文攻击下的不可区分性 (IND-CPA): 设 $\Sigma = (aKG, aEnc, aDec)$ 为基于方案 $\Pi = (KG, Enc, Dec)$ 的变形加密方案。若对任意多项式时间敌手 $\mathcal{A}$, 定义于表3中的安全游戏满足以下条件, 则称方案 Σ 满足 ND-CPA 安全性:

$$|Pr[G_{IND-CPA}^A(\lambda, 0) = 1] - Pr[G_{IND-CPA}^A(\lambda, 1) = 1]| \leq \text{negl}(\lambda)$$

表3 IND-CPA 游戏

IND-CPA 游戏 $G_{IND-CPA}^A$
1. 密钥生成算法 aKG 生成公私钥 $(apk, ask, dpk, dsk, \cdot)$
2. 调用加密谕言机 aO , 返回 $A^{aO(apk, dpk, \cdot)}(apk, ask)$, 具体流程如下:
$(msg, amsg_0, amsg_1, \cdot)$ $act_\beta \leftarrow aEnc(apk, dpk, msg, amsg_\beta, \cdot)$ 返回 $\beta \leftarrow A(act_\beta)$

定义 2.3 计算性 Diffie-Hellman (Computational Diffie-Hellman, CDH) 问题: 设 $\mathbb{G}$ 是阶数为素数的有限循环群, 给定群生成元 g 以及 g^a 和 g^b , 其中 a 和 b 是从 $\mathbb{Z}_q^*$ 中独立、均匀随机选取的未知整数, CDH 问题即计算群元素 g^{ab} 。

定义 2.4 判定性 Diffie-Hellman (Decisional Bilinear Diffie-Hellman, DBDH) 问题: 设 $\mathbb{G}$ 是阶数为素数的有限循环群, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 为对称双线性映射, g 为群生成元, $(g, A, B, C) = (g, g^a, g^b, g^c) \in \mathbb{G}^4$ 为给定元组, 其中未知指数 a, b, c 从 $\mathbb{Z}_q^*$ 中均匀随机选取, 以及一个目标群元素 $T \in \mathbb{G}_T$ 。判定 T 是双线性配对的计算结果 $e(g, g)^{abc}$, 还是目标群 $\mathbb{G}_T$ 中的一个均匀随机元素。

3 同构变形加密

3.1 同构变形加密方案

本节介绍基于 BB04 方案的同构变形加密方案。为便于阐述, 本文将变形密钥体系划分为两类: 表层密钥为监管可见的常规密钥, 底层密钥为用于隐蔽通信的变形密钥, 二者协同实现变形加密的核心功能。下面给出了初始化算法、变形密钥生成算法、变形加密算法、重构提取算法以及变形解密算法的具体步骤。

初始化阶段, 系统执行下述步骤生成参数:

(1) 输入安全参数 1^λ , 运行 Boneh-Boyen 方案的系统初始化算法 $BB.Setup(1^\lambda)$, 设 $\mathbb{G}_1$ 和 $\mathbb{G}_T$ 都为阶数为 q 的乘法群, $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ 为双线对映射, 从群 $\mathbb{G}_1$ 中随机选择生成元 (u, g, h) , 生成对称双线性群公共参数元组 $params = (\mathbb{G}_1, e, g, h, u)$, 随机从群中选取主私钥 $msk = s \in \mathbb{Z}_q^*$, 生成主公钥 $mpk = e(g, g)^s$, 定义代数映射 $G(id) = u^{id}h$ 。将其

设置为表面层的主公钥 $ampk = mpk$ 与表面层的主私钥 $amsk = msk$ 。

(2) 随机选择数值 $\alpha \leftarrow \mathbb{Z}_q^*$, 计算并设置底层主公钥 $dmpk = e(g, g)^\alpha$ 与底层主私钥 $dmsk = \alpha$, 定义哈希函数 $H: \mathbb{G}_T \rightarrow \{0, 1\}^*$ 。

(3) 输出系统的主密钥与公开参数元组 $(ampk, amsk, dmpk, dmsk)$ 。

密钥生成阶段, 可信管理者执行下述步骤生成私钥:

(1) 输入底层的主私钥 $dmsk$ 与接收者的身份标识 id 。

(2) 随机选择数值 $r \leftarrow \mathbb{Z}_q^*$ 。

(3) 计算 $d_1 = g^a (G(id))^r$ 与 $d_2 = g^r$, 并将其组合为底层身份私钥 $dsk_{id} = (d_1, d_2)$ 。

(4) 输出生成的用户底层身份私钥 dsk_{id} 。

变形加密阶段, 发送方执行下述步骤生成变形密文:

(1) 输入表层主公钥 $ampk$ 、底层主公钥 $dmpk$ 、接收者身份 id 、待加密的常规消息向量 $msg = (msg_1, msg_2)$ 以及待隐藏的变形秘密消息 $amsg$ 。

(2) 随机选择数值 $\kappa_1 \leftarrow \mathbb{Z}_q^*$, 利用常规消息 msg_1 与随机数 κ_1 , 运行标准 Boneh-Boyen 加密算法 $BB.Enc(ampk, msg_1, id; \kappa_1)$ 计算得到第一个密文组件 $act_1 = (r_1, c_{11}, c_{12})$, 其中各个分量的计算方式为: $r_1 = g^{\kappa_1}$, $c_{11} = msg_1 \cdot e(g, g)^{sk_1}$, $c_{12} = (G(id))^{\kappa_1}$ 。

(3) 利用拒绝采样技术, 随机选择 $\kappa_2 \leftarrow \mathbb{Z}_q^*$, 直到其满足以下哈希等式约束:

$$H(e(g, g)^{sk_2}) = H(e(g, g)^{sk_1}) \oplus amsg$$

(4) 利用常规消息 msg_2 与随机数 κ_2 , 运行算法 $BB.Enc(ampk, msg_2, id; \kappa_2)$, 计算第二个密文组件为 $act_2 = (r_2, c_{21}, c_{22})$, 其中各个分量为: $r_2 = g^{\kappa_2}$, $c_{21} = msg_2 \cdot e(g, g)^{sk_2}$, $c_{22} = (G(id))^{\kappa_2}$ 。

输出最终的变形密文向量 $act = (act_1, act_2)$ 。

接收方执行下述步骤提取重构密文:

(1) 输入表层身份私钥 $ask_{id} = (a_1, a_2)$ 与接收到的变形密文向量 act 。

注: 表层身份私钥由表层主私钥生成 $BB.KeyGen(amsk, id) \rightarrow ask_{id} = (g^s (G(id))^r, g^r)$ 。

(2) 解析密文向量 $act = (act_1, act_2)$, 并进一步解析出第一部分密文 $act_1 = (r_1, c_{11}, c_{12})$ 以及第二部

分密文 $act_2 = (r_2, c_{21}, c_{22})$ 。

(3) 利用 ask_{id} 计算双线性对配对以消去盲化因子并提取掩码: $\frac{e(a_1, r_2)}{e(a_2, c_{22})} = e(g, g)^{sk_2}$ 。

(4) 构建重构密文组件, 计算并设置 $\hat{r} = r_1$, $\hat{c}_1 = H(e(g, g)^{sk_2}) = H(e(g, g)^{sk_1}) \oplus amsg$, 以及 $\hat{c}_2 = (G(id))^{\kappa_1}$ 。

(5) 输出提取后的重构密文 $(\hat{r}, \hat{c}_1, \hat{c}_2)$ 。

接收方执行下述步骤恢复变形消息:

(1) 输入表层身份私钥 ask_{id} 、底层身份私钥 dsk_{id} 以及收到的变形密文向量 act 。

(2) 调用提取算法 $F(ask_{id}, act)$ 生成重构密文 $(\hat{r}, \hat{c}_1, \hat{c}_2)$, 并以此作为输入, 利用底层身份私钥 dsk_{id} 计算:

$$amsg = \hat{c}_1 \oplus H\left(\frac{e(d_1, \hat{r})}{e(d_2, \hat{c}_2)}\right)$$

输出成功恢复的原始变形消息 $amsg$ 。

3.2 安全性分析

定理 3.1 如果 DBDH 假设在双线性群中成立, 且哈希函数为随机谕言机, 那么同构变形加密方案满足变形安全性。

证明: 假设存在一个概率多项式时间敌手 $\mathcal{D}$ 能够以不可忽略的优势 ϵ 攻破该方案的变形安全性。构造一个概率多项式时间算法 $\mathcal{B}$, 该规约过程将敌手 $\mathcal{D}$ 攻破变形安全性游戏的优势转换为算法 $\mathcal{B}$ 攻破 DBDH 难题的优势。

给定 $(g, A = g^a, B = g^b, C = g^c, T)$ 为 DBDH 困难问题实例, $\mathcal{B}$ 的目标是判定 T 是否和 $e(g, g)^{abc}$ 相等。 $\mathcal{B}$ 作为挑战者, 与敌手 $\mathcal{D}$ 进行以下形式化安全游戏交互:

在系统初始化与预言机模拟阶段, $\mathcal{B}$ 随机选取表层主私钥 $s \leftarrow \mathbb{Z}_q^*$, 计算 $ampk = e(g, g)^s$, 随机选取 $x_u, x_h \leftarrow \mathbb{Z}_q^*$, 计算 $u = g^{x_u}, h = g^{x_h}$, 将 DBDH 实例参数嵌入到底层主公钥中, 底层双主私钥 $\alpha = ab$, 公开参数 $e(A, B) = e(g^a, g^b) = e(g, g)^{ab}$ 。 $\mathcal{B}$ 建立并维护随机预言机 H_2 的查询列表, 将表层主公钥 $ampk$ 、表层主私钥 $amsk$ 以及底层主公钥 $dmpk$ 发送给 $\mathcal{D}$ 。

对于 $Game_0$, 当敌手 $\mathcal{D}$ 提交目标身份 id 、常规明文向量 $msg = (msg_1, msg_2)$ 和变形明文 $amsg$ 时, 系统允许变形加密算法, 独立抽取 κ_1 , 计算 act_1 ,

然后通过拒绝采样强制抽取 κ_2 ，最后生成 act_2 。

对于 $Game_1$ ，系统直接独立且均匀地抽取真随机数 $\kappa_1, \kappa_2 \leftarrow \mathbb{Z}_q^*$ ，调用 $BB.Enc$ 生成标准的 act_1 与 act_2 。在 $Game_1$ 中，密文向量未隐藏任何变形信息。

为了区分上述两个游戏，算法 $\mathcal{B}$ 在接收到敌手 $\mathcal{D}$ 的加密询问时，将难题实例的剩余分量嵌入挑战密文：算法 $\mathcal{B}$ 隐式设定第一个底层随机数 $\kappa_1 = c$ 。算法 $\mathcal{B}$ 利用难题实例分量 $C = g^c$ 与已知的系统参数，调用 $BB.Enc$ 加密算法构造出第一部分密文组件为 $(act_1 \leftarrow BB.Enc(ampk, id, msg_1; \kappa_1))$ ，其中密文的组成部分如下： $r_1 = g^{\kappa_1} = g^c = C$ 为随机数部分， $c_{11} = msg_1 \cdot ampk^{\kappa_1} = msg_1 \cdot e(g, g)^{sk_1} = msg_1 \cdot e(C, g^s)$ 为密文的第一部分，密文的第二部分则为 $c_{12} = (G(id))^{\kappa_1} = (u^{id}h)^{\kappa_1} = (g^{x_u \cdot id} g^{x_h})^c = C^{id \cdot x_u + x_h}$ 。按照方案的代数结构，真实的隐蔽代数特征应为 $dmpk^{\kappa_1} = (e(g, g)^{ab})^c = e(g, g)^{abc}$ 。算法 $\mathcal{B}$ 使用 DBDH 难题提供的挑战元素 T 替代该隐蔽特征。算法 $\mathcal{B}$ 执行拒绝采样逻辑，不断随机抽取第二个底层随机数 $\kappa_2 \leftarrow \mathbb{Z}_q^*$ ，测试其是否满足以下代换后的约束条件： $H_2(ampk^{\kappa_2}) = amsg \oplus H_2(T)$ 算法 $\mathcal{B}$ 利用通过测试的 κ_2 调用基础加密算法生成第二部分密文 $act_2 \leftarrow BB.Enc(ampk, id, msg_2; \kappa_2)$ ，并将完整的密文向量 (act_1, act_2) 返回给 $\mathcal{D}$ 。

最终，如果 $T = e(g, g)^{abc}$ ，则 T 完美等价于真实的隐蔽代数特征。此时算法 $\mathcal{B}$ 为敌手 $\mathcal{D}$ 提供的视图在代数结构上与 $Game_0$ 绝对一致。如果 T 是目标群 $\mathbb{G}_T$ 中的均匀随机元素，在随机预言机模型下，未被查询过的输入点 T 的输出值 $H_2(T)$ 在有限域内服从绝对的均匀分布。因此， $amsng \oplus H_2(T)$ 为一个均匀随机串。这使得等式 $H_2(ampk^{\kappa_2})$ 为随机串，失去了原本的代数约束力，致使筛选出的 κ_2 在敌手的视图中表现为完美均匀分布的真随机数，此视图完美等价于独立抽取双随机数的 $Game_1$ 。

定理 3.2 如果 DBDH 假设在双线性群中成立，且哈希函数为随机谰言机，那么同构变形加密方案满足 IND-CPA 安全性。

证明： 构建一个概率多项式时间的模拟器 $\mathcal{C}$ ，假设存在一个能够以不可忽略的优势 ϵ 赢得 IND-CPA 游戏的敌手 $\mathcal{A}$ ，那么 $\mathcal{C}$ 就可以利用 $\mathcal{A}$ 的能力，以相同的优势解决 DBDH 难题。 $\mathcal{C}$ 将作为挑战者，与 $\mathcal{A}$ 依次执行以下 IND-CPA 安全游戏交互。

在初始化阶段， $\mathcal{C}$ 运行系统初始化算法生成公共参数，并将 DBDH 实例隐蔽地嵌入到底层主公钥中。首先， $\mathcal{C}$ 随机选取表面层主私钥 $s \leftarrow \mathbb{Z}_q^*$ ，计算表面层主公钥 $ampk = e(g, g)^s$ 。 $\mathcal{C}$ 可以响应关于表面层解密私钥 ask_{id} 的查询。接着， $\mathcal{C}$ 隐式设定底层主私钥为 $a = ab$ ，利用双线性配对计算出底层主公钥 $dmpk = e(A, B) = e(g^a, g^b) = e(g, g)^{ab}$ ，采用 Boneh-Boyen 方案的标准模拟策略来构造代数映射 $G(id)$ 。随后， $\mathcal{C}$ 将全局公共参数 $params$ 、表面层主公钥 $ampk$ 以及底层主公钥 $dmpk$ 发送给 $\mathcal{A}$ ，同时建立并维护随机预言机哈希函数 H 的查询列表。

在第一阶段询问中， $\mathcal{A}$ 可以自适应地向预言机发起底层变形密钥 dsk_{id_i} 的查询。由于 r_i 是均匀随机的，生成的 dsk_{id_i} 在概率分布上与真实私钥不可区分， $\mathcal{C}$ 将其返回给 $\mathcal{A}$ 。

随后进入挑战阶段， $\mathcal{A}$ 选定一个目标身份 id^* 、一个常规明文向量，以及两个变形消息。 $\mathcal{C}$ 随机抛掷硬币选取 $\beta \in \{0, 1\}$ ，第一个密文组件的随机数 $\kappa_1 = c$ ， $r_1 = C = g^{\kappa_1}$ 、 $c_{11} = msg_1 \cdot e(C, g^s) = msg_1 \cdot e(g, g)^{sk_1}$ $c_{12} = C^{id^* \cdot x_u + x_h} = (G(id^*))^{\kappa_1}$ 。在加密过程中，底层代数特征应为 $(dmpk)^{\kappa_1} = e(g, g)^{abc}$ ，由于 $\mathcal{C}$ 不知道 a, b, c ，则使用 DBDH 难题中提供的待判定元素 T 来替代该隐蔽特征， $\mathcal{C}$ 执行拒绝采样逻辑，不断随机抽取 $\kappa_2 \leftarrow \mathbb{Z}_q^*$ ，直到其满足哈希约束，找到合适的 κ_2 后，利用掌握的 s 和正常的加密逻辑计算出第二部分密文 act_2 ，即 $r_2 = g^{\kappa_2}$ 、 $c_{21} = msg_2 \cdot e(g, g)^{sk_2}$ 以及 $c_{22} = (G(id^*))^{\kappa_2}$ 。最后， $\mathcal{C}$ 将组合好的最终挑战密文 $act^* = (act_1, act_2)$ 发送给 $\mathcal{A}$ 。在第二阶段询问中， $\mathcal{A}$ 收到挑战密文后可以继续发起底层密钥询问。 $\mathcal{C}$ 按照第一阶段的方式进行响应。

最终进入猜测与优势分析阶段， $\mathcal{A}$ 输出一个猜测比特 β' 。 $\mathcal{C}$ 根据 $\mathcal{A}$ 的猜测来解答 DBDH 难题：如果 $\beta' = \beta$ ， $\mathcal{C}$ 输出 1，即判定 $T = e(g, g)^{abc}$ ；如果 $\beta' \neq \beta$ ， $\mathcal{C}$ 输出 0，即判定 T 是随机元素。如果 DBDH 实例中的 $T = e(g, g)^{abc}$ ，此时替代元素 T 在代数上等价于真实的隐蔽特征 $(dmpk)^{\kappa_1}$ ， $\mathcal{C}$ 为 $\mathcal{A}$ 提供的挑战密文分布与真实的 IND-CPA 游戏分布绝对一致。根据假设， $\Pr[\beta' = \beta | T = e(g, g)^{abc}] = 1/2 + \epsilon$ 为 $\mathcal{A}$ 赢得游戏的概率。反之，如果 DBDH 实例中的 T 是目标群 $\mathbb{G}_T$ 中的均匀随机元素，由于哈希函数 H 被建模为随机预言机，未被查询过的随

机输入点 T 对应的输出 $H(T)$ 在有限域内表现为均匀随机比特串。此时, $\mathcal{A}$ 猜测正确的概率等于 $\Pr[\beta' = \beta] = 1/2$ 。综合上述两种情形, $\mathcal{C}$ 解决 DBDH 难题的优势为 $Adv_c^{DBDH} = |(1/2 + \epsilon) - 1/2| = \epsilon$ 。由于在多项式时间内攻破 DBDH 假设是困难的, 因此 ϵ 是一个可忽略函数, 由此证明该同构变形加密方案实例满足 IND-CPA 安全性。

4 异构变形加密

4.1 异构变形加密方案

本文选取 ElGamal 作为表层公钥加密实例, 核心原因是其代数结构与底层身份基加密机制兼容。本文去中心化体现在无证书机制中, 用户私钥由密钥生成中心生成的部分私钥与用户本地自选秘密共同构造, 消除单点托管风险。若主密钥泄露, 因攻击者缺乏用户本地秘密, 仍无法还原完整私钥, 变形通道的隐蔽性与安全性依然成立。

下面介绍异构变形加密方案的具体实现。

初始化算法。系统执行下述步骤生成全局参数与底层主密钥:

(1) 输入安全参数 1^t , 选择大素数 p 和 q , 满足 q 整除 $p - 1$ 。设 $\mathbb{G}$ 为阶为 q 的乘法循环群, g 为群 $\mathbb{G}$ 的生成元。定义哈希函数 $H_1: \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $H_2: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$ 。

(2) 生成底层隐蔽主密钥: 密钥生成中心运行底层 CLPKE 方案的初始化算法, 随机选择数值 $\alpha \in \mathbb{Z}_q^*$, 生成底层隐蔽主公钥 $dmpk = g^\alpha$ 以及底层主私钥 $dmsk = \alpha$, 秘密保存主私钥 $dmsk$ 。

(3) $params = (p, q, \mathbb{G}, g, dmpk, H_1, H_2)$ 为公共参数。

密钥生成算法。密钥生成中心与用户交互, 生成表面的常规密钥与底层的隐蔽双密钥:

(1) 生成表面常规密钥: 用户在本地随机选择 $x \in \mathbb{Z}_q^*$ 作为表层私钥 $ask = x$, 计算表层公钥 $apk = y = g^x$ 。

(2) 提取部分密钥: 密钥生成中心输入底层主私钥 $dmsk$ 与用户的身份标识 id , 随机选择 $s \in \mathbb{Z}_q^*$, 计算 $w = g^s$ 与 $t = s + \alpha H_1(id, w)$, 生成并给用户分发部分公私钥对 $(P_{id}, D_{id}) = (w, t)$ 。

(3) 设置底层身份密钥对: 隐蔽接收者随机选择 $z \in \mathbb{Z}_q^*$ 作为秘密值, 将其与部分私钥结合构成最

终的底层身份私钥 $dsk_{id} = (z, t) = (z, s + \alpha H_1(id, w))$; 同时计算 $\eta = g^z$, 将其与部分公钥结合构成最终的底层身份公钥 $dpk_{id} = (w, \eta) = (g^s, g^z)$ 。

变形加密算法。发送方执行下述步骤生成异构变形密文:

(1) 输入表层公钥 apk 、接收者底层身份公钥 dpk_{id} 、底层主公钥 $dmpk$ 、接收者身份 id 、待隐藏的变形消息 $amsg$ 、待加密的常规消息向量 $msg = (msg_1, msg_2)$ 。

(2) 针对常规消息 msg_1 , 随机选择 $\mu_1 \in \mathbb{Z}_q$, 执行 ElGamal 加密算法计算 $r_1 = g^{\mu_1}$ 与 $c_1 = apk^{\mu_1} \cdot msg_1$, $act_1 = (r_1, c_1)$ 为第一部分变形密文组件。

(3) 调用底层 CLPKE 方案的密钥封装机制: 输入底层身份公钥 dpk_{id} 、随机数 μ_1 与底层主公钥 $dmpk$, 计算 $k_1 = \eta^{\mu_1} = g^{z\mu_1}$, $\gamma_{id} = w \cdot dmpk^{H_1(id, w)}$ 以及 $k_2 = \gamma_{id}^{\mu_1}$ 。随后计算 $\mu_2 = H_2(k_1, k_2) \cdot amsg \pmod{q}$ 嵌入变形消息, 将 μ_2 设定第二次加密的随机数。

(4) 针对常规消息 msg_2 , 利用 μ_2 , 执行 ElGamal 加密算法计算 $r_2 = g^{\mu_2}$ 与 $c_2 = apk^{\mu_2} \cdot msg_2$, $act_2 = (r_2, c_2)$ 为第二部分变形密文组件。

输出最终的变形密文向量 $act = (act_1, act_2)$ 。

变形解密算法。隐蔽接收者执行下述步骤恢复变形消息:

(1) 输入接收者的双私钥 $dsk_{id} = (z, t)$ 以及接收到的变形密文向量 act 。

(2) 密文组件为 $act_1 = (r_1, c_1)$ 与 $act_2 = (r_2, c_2)$, 从 act_1 中提取底层随机数元素 $r_1 = g^{\mu_1}$ 。

(3) 提取身份私钥 dsk_{id} 得到 z 和 t , 利用 $r_1 = g^{\mu_1}$ 重新计算 $H_2(r_1^z, r_1^t) = H_2(g^{z\mu_1}, g^{t\mu_1})$ 。

(4) 提取 act_2 中的 r_2 , 计算哈希掩码在模 q 下的乘法逆元, 并执行指数求幂运算以消去盲化掩码, 恢复变形消息的映射群元素: $\hat{m} = r_2^{(H_2(k_1, k_2))^{-1}}$ 。

(5) 遍历多项式大小的变形消息空间 $\hat{\mathcal{M}}$, 通过查找表 T (该表将 g^{amsg} 映射到 $amsg$)。在表中查找到匹配的 $\hat{m}$, 提取其对应的原像即为变形消息 $amsg$ 。

输出成功恢复的变形消息 $amsg$ (若未找到匹配项则输出终止符号 $\perp$)。

4.2 安全性分析

定理 4.1 如果 CDH 困难问题成立, 并且哈希函数 H_2 为随机谕言机, 那么异构变形加密方案满足变形安全性。

证明: 假设存在一个概率多项式时间敌手 $\mathcal{A}$ 能够以不可忽略的优势区分真实游戏 $RealG_{\mathcal{A}}(\lambda)$ 与变形游戏 $AnamG_{\mathcal{A}}(\lambda)$ 。构造一个概率多项式时间算法 $\mathcal{B}$, 该规约游戏将敌手 $\mathcal{A}$ 攻破变形安全性游戏的优势转换为算法 $\mathcal{B}$ 攻破 CDH 难题的优势。给定 CDH 困难问题实例 (g, g^a, g^b) , $\mathcal{B}$ 的目标是计算出 g^{ab} 。 $\mathcal{B}$ 模拟挑战者将与敌手 $\mathcal{A}$ 进行以下交互。

在系统初始化与密钥生成阶段, 算法 $\mathcal{B}$ 隐式地设定隐蔽双公钥中的参数 $\eta = g^a$ 。 $\mathcal{B}$ 选择表面常规私钥 $ask = x$, 并计算表面常规公钥 $apk = g^x$ 。 $\mathcal{B}$ 正常生成底层身份公钥的剩余分量 w 以及底层主公钥 $dmpk$ 。 $\mathcal{B}$ 将公共参数、 $dpk_{id} = (w, \eta)$ 、 apk 以及 $ask = x$ 发送给敌手 $\mathcal{A}$ 。

在 $RealG_{\mathcal{A}}(\lambda)$ 真实游戏中, 当 $\mathcal{A}$ 提交包含常规掩护消息向量 $msg = (msg_1, msg_2)$ 和变形秘密消息 $amsmsg$ 的加密询问时, $\mathcal{B}$ 将 CDH 实例嵌入第一部分密文中。 $\mathcal{B}$ 隐式地设定第一部分密文的随机数 $\mu_1 = b$, 计算密文组件 $act_1 = (g^b, (g^b)^x \cdot msg_1)$ 。算法 $\mathcal{B}$ 独立且均匀地选取真随机数 $\mu_2 \in \mathbb{Z}_q^*$, 计算密文组件 $act_2 = (g^{\mu_2}, apk^{\mu_2} \cdot msg_2)$ 。算法 $\mathcal{B}$ 将密文向量 $act = (act_1, act_2)$ 返回给 $\mathcal{A}$ 。在 $AnamG_{\mathcal{A}}(\lambda)$ 变形游戏中, $\mathcal{B}$ 改变第二次加密中随机数 μ_2 的生成方式。 $\mathcal{B}$ 设定 $\mu_2 = H_2(k_1, k_2) \cdot amsmsg \pmod{q}$, 并利用该特定的代数值计算密文组件 act_2 。在随机谕言机模型下, 除非 $\mathcal{A}$ 向 H_2 提交了正确的查询元组 (k_1, k_2) , 否则 $H_2(k_1, k_2)$ 的输出值在有限域 $\mathbb{Z}_q^*$ 中服从绝对的均匀分布。在有限乘法群 $\mathbb{Z}_q^*$ 中, 一个完全均匀分布的随机变量乘以任何固定的常数 $amsmsg$, 其结果 μ_2 依然服从绝对的均匀分布。此时构造的 μ_2 与 $RealG_{\mathcal{A}}(\lambda)$ 中均匀抽取的 μ_2 在统计分布上完美不可区分。

$\mathcal{B}$ 持续监控敌手 $\mathcal{A}$ 对 H_2 发起的所有查询列表。底层代数参数 k_1 的精确代数值为 $\eta^{\mu_1} = (g^a)^b = g^{ab}$ 。如果 $\mathcal{A}$ 能够以不可忽略的优势区分 $RealG_{\mathcal{A}}(\lambda)$ 与 $AnamG_{\mathcal{A}}(\lambda)$, 意味着 $\mathcal{A}$ 以不可忽略的概率向 H_2 提交了包含正确代数参数 k_1 的查询。 $\mathcal{B}$ 检查查询列

表, 提取出匹配的查询输入 K_1 , 并将其作为 CDH 的解 g^{ab} 输出。该规约过程将 $\mathcal{A}$ 攻破变形安全性游戏的优势完美转换为 $\mathcal{B}$ 攻破 CDH 困难问题的优势。最终 $\mathcal{B}$ 成功破解了 CDH 难题, 然而在多项式时间内破解 CDH 问题是困难的, 故产生矛盾。因此 $\mathcal{A}$ 无法区分 $RealG_{\mathcal{A}}(\lambda)$ 与 $AnamG_{\mathcal{A}}(\lambda)$, 异构变形加密方案满足变形安全性。

定理 4.2 如果 CDH 困难问题在群 $\mathbb{G}$ 中成立, 并且将哈希函数 H_2 建模为随机谕言机, 那么异构变形加密方案满足 IND-CPA 安全性。

证明: 假设存在一个概率多项式时间敌手 $\mathcal{A}$ 能够以不可忽略的优势 ϵ 攻破该方案的 IND-CPA 安全性。构造一个概率多项式时间算法 $\mathcal{B}$, 该规约过程将敌手 $\mathcal{A}$ 攻破变形安全性游戏的优势转换为算法 $\mathcal{B}$ 攻破 CDH 难题的优势。

给定 CDH 难题实例 $(g, A = g^a, B = g^b)$, $\mathcal{B}$ 的计算目标是输出 g^{ab} 。 $\mathcal{B}$ 作为挑战者, 与 $\mathcal{A}$ 进行以下形式化安全游戏交互:

$\mathcal{B}$ 在系统与密钥初始化阶段, 选取 $\alpha \in \mathbb{Z}_q^*$, 计算底层主公钥 $dmpk = g^a$ 。 $\mathcal{B}$ 选取 $x \in \mathbb{Z}_q^*$, 计算表层常规公钥 $apk = g^x$, 建立并维护一个初始为空的哈希查询记录列表 L_{H_2} , 将公开参数 $params$ 、底层主公钥 $dmpk$ 以及表层常规公钥 apk 发送给 $\mathcal{A}$ 。

在随机谕言机模拟阶段, $\mathcal{A}$ 提交对哈希函数 $H_2(K_1, K_2)$ 的自适应查询。 $\mathcal{B}$ 检索记录列表 L_{H_2} 。若查询元组已存在, 直接返回对应的历史结果。若查询元组不存在, $\mathcal{B}$ 独立选取随机数 $R \in \mathbb{Z}_q^*$, 将元组 (K_1, K_2, R) 存入记录列表 L_{H_2} , 并将 R 返回给 $\mathcal{A}$ 。在询问阶段, $\mathcal{A}$ 提交目标身份 id_i 发起隐蔽密钥提取询问。 $\mathcal{B}$ 利用自身掌握的底层隐蔽主私钥 α 执行异构密钥生成算法, 生成对应的 dpk_{id_i} 与 dsk_{id_i} , 并将其返回给 $\mathcal{A}$ 。在挑战阶段, $\mathcal{A}$ 输出目标身份 id^* 、常规消息向量 $msg = (msg_1, msg_2)$, 以及两段长度相等的变形消息 $amsmsg_0$ 和 $amsmsg_1$ 。 $\mathcal{A}$ 被限制对目标身份 id^* 发起询问。 $\mathcal{B}$ 将 CDH 难题实例的代数参数嵌入到目标身份 id^* 的底层身份公钥与挑战密文之中, 隐式设定目标底层身份公钥的代数分量 $\eta^* = A = g^a$ (即隐式设定目标底层身份私钥分量 $z^* = a$), 随机选择一个挑战比特 $\beta \in \{0, 1\}$, 同时隐式设定第一部分密文的底层随机数 $\mu_1 = b$ 。 $\mathcal{B}$ 利用困难问题实

例分量 $B = g^b$ 与表面常规私钥 x , 直接计算第一部分挑战密文 $act_1^* = (B, B^x \cdot msg_1)$ 。此时, 方案底层的隐蔽代数参数 k_1 精确映射为 $(\eta^*)^{\mu_1} = (g^a)^b = g^{ab}$ 。由于算法 $\mathcal{B}$ 在该阶段尚未获取 g^{ab} , 无法查询随机谕言机得到合法的哈希掩码。算法 $\mathcal{B}$ 采取完美隐藏模拟策略, 直接独立选取纯随机数 $\mu_2 \in \mathbb{Z}_q^*$, 计算第二部分挑战密文 $act_2^* = (g^{\mu_2}, apk^{\mu_2} \cdot msg_2)$, 将 $act_\beta = (act_1^*, act_2^*)$ 返回给敌手 $\mathcal{A}$ 。

在询问阶段 2, $\mathcal{A}$ 继续发起底层身份密钥提取询问。在随机谕言机模型下, 算法 $\mathcal{B}$ 选取的纯随机数 μ_2 在有限域 $\mathbb{Z}_q^*$ 内服从绝对的均匀分布。事件 E 表示 $\mathcal{A}$ 向随机谕言机 H_2 提交包含 $k_1 = g^{ab}$ 的查询。若 E 未发生, 由于随机谕言机输出的绝对均匀随机性与有限域乘法的掩盖性, 第二部分挑战密文中的随机数 μ_2 在敌手视角下独立服从均匀分布, 对 $\mathcal{A}$ 构成信息论意义上的完美隐藏。此时 $\mathcal{A}$ 猜中 β 的条件概率满足 $\Pr[\text{Win} | \neg E] = 1/2$ 。根据全概率公式, $\mathcal{A}$ 的区分优势满足 $\epsilon = |\Pr[\text{Win}] - 1/2| \leq \Pr[E]/2$, 进而导出概率下界 $\Pr[E] \geq 2\epsilon$ 。由此推导可知, 若 $\mathcal{A}$ 能获得不可忽略的优势 ϵ , 其向 H_2 提交包含 $k_1 = g^{ab}$ 的查询概率必然不低于 2ϵ 。游戏交互结束时, 算法 $\mathcal{B}$ 截获敌手 $\mathcal{A}$ 的哈希查询记录列表 L_{H_2} 。算法 $\mathcal{B}$ 从该列表中随机抽取一个历史查询输入分量 K_1 , 将其作为 CDH 难题实例的计算解输出。假设 $\mathcal{A}$ 发起的最大哈希查询次数为多项式有界值 q_{H_2} , $\mathcal{B}$ 从列表中成功命中并输出正确解 g^{ab} 的概率至少为 ϵ/q_{H_2} 。该规约验证过程将 $\mathcal{A}$ 攻破 IND-CPA 安全性游戏的优势, 转换为 $\mathcal{B}$ 攻破 CDH 难题的优势。得出结论 $\mathcal{A}$ 在多项式时间内成功协助 $\mathcal{B}$ 攻破了 CDH 难题。而破解 CDH 难题是困难的, 规约推导在此产生矛盾。故 $\mathcal{A}$ 无法在多项式时间内区分游戏中的挑战密文, 异构变形加密方案满足 IND-CPA 安全性。

5 性能评估

5.1 时间开销

为评估本章方案在不同比特安全等级下的效率, 配备了如下的实验设备: 64 位的 Windows10 操作系统, 使用 8GB 的 RAM、1.60GHz 的处理器以及 i5-8265 的 CPU 进行试验, 基于 Charm 密码学库及 Python 编程语言实现各算法, 每项加密测试

表 4 不同安全等级下异构方案相关操作平均消耗时间(毫秒)

符号	描述	80 比特安全	112 比特安全	128 比特安全
T_{G-A}	群 G 中的加法操作	0.0006	0.0007	0.0007
T_{G-M}	群 G 中的标量乘法操作	0.1906	0.2991	0.4076
T_{Z-A}	群 $\mathbb{Z}_q^*$ 中的加法操作	0.0095	0.0101	0.0106
T_{Z-M}	群 $\mathbb{Z}_q^*$ 中的乘法操作	0.0099	0.0104	0.0108
T_E	ElGamal 加密操作	0.9066	1.6080	2.3094
T_D	ElGamal 解密操作	0.3258	1.3567	2.3875

表 5 不同安全等级下同构方案相关操作平均消耗时间(毫秒)

符号	描述	80 比特安全	112 比特安全	128 比特安全
T_e	群 G_1 中的指数操作	0.8368	2.645	4.6956
T_a	群 G_1 中的加法操作	0.0029	0.0073	0.0099
T_{e_G}	群 G_T 中的指数操作	0.0712	0.2285	0.4951
T_{em}	群 G_T 中的乘法操作	0.0031	0.0122	0.0274
T_p	双线性配对操作	0.5314	2.5012	5.6465
T_H	哈希映射操作	0.0039	0.0055	0.0078

均重复执行 1000 次并记录平均时间。表 4 为该实验设备分别在 80 比特、112 比特、128 比特安全性下, 执行异构方案相关操作平均消耗时间, 表 5 为该实验设备分别在 80 比特、112 比特、128 比特安全性下, 执行同构方案相关操作平均消耗时间, 单位均为毫秒。

方案[11]与本文方案同属极端监控场景下的身份基变形加密研究, 图 1 对比了方案[11]、同构方案和异构方案在 80 比特安全性下各个算法的计算代价, 综合密钥生成、加解密总耗时, 本文异构方案总代价最低, 较现有方案优势明显, 整体性能高效, 适配强监管场景。表 6 给出了不同安全等级下, 各个方案的总体计算代价, 异构方案表层采用常规公钥加密架, 整体计算代价最低。同构方案依赖复杂的双线性对映射运算, 计算复杂度高且随安全等级提升剧增。

5.2 通信开销

图 2 对比了方案[11]、同构方案和异构方案随着变形用户增加通信代价的变化, 虽然异构方案的通信代价与方案[11]对比有所增加, 但异构方案通过增加少量的参数, 为变形消息开辟了更大的空

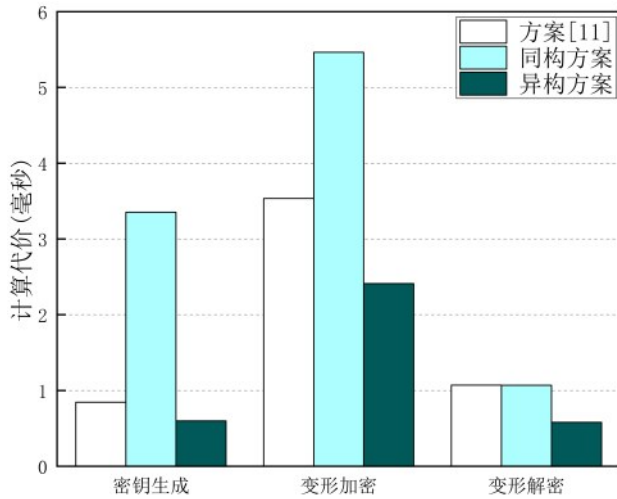


图1 80比特安全等级下不同方案的计算代价

间,从而支持更长的变形消息的嵌入,通信代价的增加本质上是为换取更高的嵌入密度与对变形用户组更强的管理。

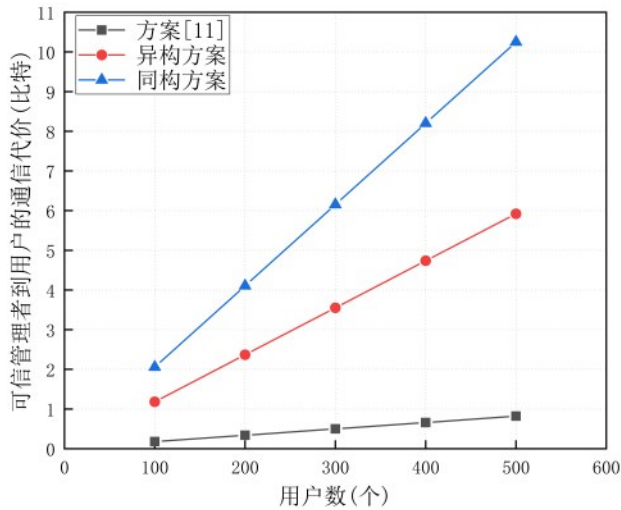


图2 80比特安全等级下不同方案的通信代价

6 结束语

本文面向弱监管与强监管两类不同的监管机制,系统性地提出了两种不同的身份基变形加密方案,其中同构变形加密方案依托同类身份基加密方案的结构自相似性,无需复杂嵌套即可提取变形消息,而异构变形加密方案兼容标准公钥加密体系以满足监管合规,又可构建隐蔽通信通道保护用户隐私,降低了对单一管理者的信任依赖。最后,本文通过安全性证明与性能分析验证了两类方案的有效性与可行性。

表6 不同方案总体计算代价比较(毫秒)

算法	方案[11]	同构方案	异构方案
密钥生成	$T_e + T_H$	$4T_e + 2T_a$	$3T_{G-M} + T_{Z-A} + T_{Z-M} + T_H$
变形加密	$2T_p + 2T_e + 2T_{e_G} + 3T_H + 2(T_{e_G} + T_H)$	$5T_e + T_{e_G} + T_{em} + T_a + 4(T_{e_G} + T_H)$	$3T_{G-M} + 2T_E + 2T_H + T_{Z-M} + T_{G-A}$
变形解密	$2T_p + 2T_H$	$2T_p + T_{em} + T_H$	$3T_{G-M} + T_H$
总体代价(80bit)	5.4494	9.8861	3.5897
总体代价(112bit)	8.1824	32.8307	5.5891
总体代价(128bit)	10.8932	129.3952	7.6083

赵一 (1985-), 男, 博士, 长安大学副教授, 主要研究方向为公钥密码学、可证明安全性、隐私保护、区块链、多方安全计算协议等。

[作者简介]



明洋 (1979-), 男, 博士, 长安大学教授, 主要研究方向为数据安全和隐私、车联网安全和隐私、云计算安全和隐私、人工智能安全等。

[作者简介]



李思琦 (2001-), 女, 长安大学硕士生, 主要研究方向为网络安全、公钥密码学、后门攻击等。



张启福 (2001-), 男, 长安大学硕士, 主要研究方向为公钥密码学、可证明安全、隐私保护等。



- [22] K[23][24][25][26] utylowski M, Persiano G, Phan D H, et al. Anamorphic signatures: Secrecy from a dictator who only permits authentication! [A]. In Proceedings of Advances in Cryptology-CRYPTO'24[C]. Berlin: Springer, 2023: 759-790.[27] Catalano D, Giunta E, Migliaro F. Generic anamorphic encryption, revisited: new limitations and constructions [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'25[C]. Berlin: Springer, 2025: 275-303.[28] Persiano G, Phan D H, Yung M. Public-key anamorphism in (CCA-secure) public-key encryption and beyond [A]. In Proceedings of Advances in Cryptology-CRYPTO'24[C]. Berlin: Springer, 2024: 422-455.[29] Jaeger J, Stracovsky R. Dictators? Friends? Forgers. Breaking and Fixing Unforgeability Definitions for Anamorphic Signature Schemes [A]. In Proceedings of Advances in Cryptology-ASIACRYPT'23[C]. Berlin: Springer, 2024: 105-137.[30] Chu H, Do K, Hanzlik L, et al. When Threshold Meets Anamorphic Signatures: What is Possible and What is Not! [J]. Cryptology ePrint Archive, 2025: 1044.[31] Do X T, Persiano G, Phan D H, et al. Anamorphism beyond one-to-one messaging: Public-key with anamorphic broadcast mode [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'25[C]. Berlin: Springer, 2025: 429-455.[32] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing [A]. In Proceedings of International conference on information security[C]. Berlin: Springer, 2005: 134-148

参考文献:

- [1] Persiano G, Phan D H, Yung M. Anamorphic encryption: private communication against a dictator [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'22[C]. Berlin: Springer, 2022: 34-63.
- [2] Young A, Yung M. Kleptography: Using cryptography against cryptography [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'97 [C]. Cham: Springer, 1997: 62-74.
- [3] Young A, Yung M. Malicious cryptography: Kleptographic aspects [A]. In Proceedings of Cryptographers' Track at the RSA Conference[C]. Cham: Springer, 2005: 7-18.
- [4] Young A, Yung M. A space efficient backdoor in RSA and its applications [A]. In Proceedings of International Workshop on Selected Areas in Cryptography[C]. Cham: Springer, 2005: 128-143.
- [5] Wong D. How to backdoor diffie-hellman [J]. Cryptology ePrint Archive, 2016: 644.
- [6] Young A, Yung M. The dark side of "black-box" cryptography or: Should we trust capstone? [A]. In Proceedings of Advances in Cryptology-CRYPTO'96[C]. Berlin: Springer, 1996: 89-103.
- [7] Young A, Yung M. The prevalence of kleptographic attacks on discrete-log based cryptosystems [A]. In Proceedings of Advances in Cryptology-CRYPTO'97[C]. Cham: Springer, 1997: 264-276.
- [8] Von Ahn L, Hopper N J. Public-key steganography [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'04[C]. Cham: Springer, 2004: 323-341.
- [9] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [A]. In Proceedings of Advances in Cryptology-CRYPTO'01[C]. Berlin: Springer, 2001: 213-229.
- [10] BONEH D, BOYEN X. Efficient selective-ID secure identity based encryption without random oracles [C]. Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 223-238.
- [11] Banerjee S, Pal T, Rupp A, et al. Simple Public Key Anamorphic Encryption and Signature using Multi-Message Extensions [J]. IACR

- Cryptol ePrint Arch, 2025, 2025: 370.
- [12] Wang Y, Chen R, Huang X, et al. Sender-anamorphic encryption reformulated: Achieving robust and generic constructions [A]. In Proceedings of Advances in Cryptology-ASIACRYPT'22[C]. Berlin: Springer, 2023: 135-167.
- [13] Choi W, Collins D, Liu X, et al. A unified treatment of anamorphic encryption [J]. Cryptology ePrint Archive, 2025: 309.
- [14] Kutyłowski M, Persiano G, Phan D H, et al. The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography [J]. Proceedings on Privacy Enhancing Technologies, 2023, 2023(4): 170-183.
- [15] Banfi F, Gegier K, Hirt M, et al. Anamorphic encryption, revisited [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'23[C]. Berlin: Springer, 2024: 3-32.
- [16] Catalano D, Giunta E, Migliaro F. Anamorphic encryption: New constructions and homomorphic realizations [A]. In Proceedings of Advances in Cryptology-EUROCRYPT'24[C]. Berlin: Springer, 2024: 33-62.
- [17] Wang W, Han S, Liu S. Anamorphic authenticated key exchange: Double key distribution under surveillance [A]. In Proceedings of Advances in Cryptology-ASIACRYPT'23[C]. Berlin: Springer, 2024: 168-200.
- [18]
- [19]
- [20]
- [21]