基于 SM9 的可验证公平标识广播代理重加密

刘 行 明 洋 王晨豪 赵 一
（长安大学信息工程学院 西安 710018）

摘 要 标识广播代理重加密允许代理者将数据拥有者的密文转换为一组授权用户可解的密文且不泄露底层的数据和私钥，解决证书管理问题，实现一对多密文转换，有效地适配于多用户数据共享系统。然而，负责转换密文的不可信代理者可能为节省计算开销返回错误重加密密文导致数据共享失败。SM9 算法作为我国自主设计的标识密码，在实现隐私保护的同时具有更高效率，但其不支持密文转换且仅适用于一对一共享场景。针对上述问题，本文基于 SM9 标识加密算法，提出一种可验证公平标识广播代理重加密方案。该方案中用户私钥与 SM9 算法一致，与现有 SM9 系统能够高效融合。重加密密钥和重加密密文长度保持恒定，与授权用户数量无关，显著降低系统通信开销。基于 Fujisaki-Okamoto 转换思想和零知识证明协议，所提方案能够同时实现可验证性和公平性，前者保证授权用户能够在解密的同时验证不可信代理者是否诚实转换密文，后者确保代理者在诚实转换时免受恶意追责。本文优化可验证公平标识广播代理重加密的形式化定义及安全模型，在随机预言机下证明所提方案能够抵抗静态选择明文攻击和合谋攻击。性能分析表明，相比于已知方案，所提方案取得了更低的计算代价和存储代价。

关键词 SM9；标识广播代理重加密；可验证性；公平性；云存储
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2025.00721

Verifiable and Fair Identity-Based Broadcast Proxy Re-Encryption Based on SM9

LIU Hang MING Yang WANG Chen-Hao ZHAO Yi
(School of Information Engineering, Chang'an University, Xi'an 710018)

Abstract Identity-based broadcast proxy re-encryption (IBBPRE) enables the proxy to transform the ciphertext of the data owner into a ciphertext that can be decrypted by a set of authorized users without revealing the underlying data and private key, solves the certificate management problem of proxy re-encryption, and achieves one-to-many ciphertext transformation, thus effectively adapting to the multi-user data sharing system. The availability of IBBPRE is built upon the honest execution of re-encryption (i.e., ciphertext transformation) operations by the proxy. However, the untrusted proxy deployed by a third party is likely to generate incorrect re-encrypted ciphertexts in order to save local storage space and computation overhead, which leads to data sharing failure. SM9 series algorithms, as independently designed identity-based cryptography, have higher efficiency while realizing privacy protection. At present, the SM9 series algorithms have become national standards and ISO/IEC international standards, with an increasingly important status. However, the SM9 identity-based encryption algorithm does not support ciphertext transformation and is only applicable to single-user scenarios. To overcome the aforementioned problems, this paper presents a verifiable and fair identity-based broadcast proxy re-encryption (VF-IBBPRE) scheme on the basis of the SM9 identity-based encryption

收稿日期：2024-04-12；在线发布日期：2024-12-05. 本课题得到国家自然科学基金(62472049，62072054)、陕西省重点研发计划(2024GX-YBXM-078)、西安市科技计划(23ZDCYJSGG0009-2022)、中央高校基本科研业务费专项资金(300102242201)资助。**刘 行**，博士研究生，主要研究方向为公钥密码学、数据共享安全。E-mail：hangliu@chd.edu.cn。**明 洋**(通信作者)，博士，教授，博士生导师，中国计算机学会(CCF)会员，主要研究领域为密码学、信息安全。E-mail：yangming@chd.edu.cn。**王晨豪**，博士研究生，主要研究领域为公钥密码学、数字孪生安全。**赵 一**，博士，讲师，主要研究方向为密码学、网络安全。

algorithm, making the data owner share the data with a set of authorized users in a secure and verifiable manner. The proposed scheme is consistent with the SM9 algorithm in the user's private key, so it can be efficiently integrated with the existing SM9 system. The size of the re-encryption key and re-encrypted ciphertext remain constant and independent of the number of authorized users, significantly reducing the system communication overhead and storage cost. Inspired by the idea of the Fujisaki-Okamoto transformation, the proposed scheme integrates the data into the random number which does not require an additional generation of commitments, providing verifiability for the authorized users (i.e., ensuring that the authorized users can verify whether the untrusted proxy transforms the ciphertext honestly while decrypting the ciphertext). Meanwhile, by designing an efficient zero-knowledge proof protocol, the proposed scheme guarantees that the proxy is free from malicious accusations when it performs the transformation honestly, thus offering fairness for the proxy. Furthermore, we optimize the formal definition and security model for VF-IBBPRE. Specifically, in our definition, the verification phase can be performed publicly with no need to involve the original ciphertext and re-encryption key, which reduces the communication overhead and guarantees the security of the re-encryption key. In random oracle model, based on General Decisional Diffie-Hellman Exponent, q-Strong Diffie-Hellman, hash function collision resistance assumptions and the soundness of zero-knowledge proof protocol, the proposed scheme is formally proved to secure against selective identity and chosen plaintext attacks and collusion attacks while achieving verifiability and fairness. A comprehensive analysis of theoretical and experimental results demonstrates that, in comparison with existing schemes, the proposed scheme significantly reduces the computational cost of re-encryption key generation and re-encrypted ciphertext decryption, thereby greatly reducing the computational cost of the user and the cloud server on the basis of achieving complete verifiability. Meanwhile, the proposed scheme achieves a more favorable storage cost and is more feasible for cloud storage.

Keywords SM9; identity-based broadcast proxy re-encryption; verifiability; fairness; cloud storage

1 引 言

随着云计算的发展,云存储作为一种新兴网络存储技术,为企业和用户提供了便捷的按需分配的数据存储服务[1]。目前,越来越多的数据存储在云服务器上从而释放本地资源。然而,云服务器是由不可信的第三方进行管理维护的,导致存在严重的数据安全和隐私威胁[2-3]。该问题的直接解决方法是采用加密后外包范式[4-5]。然而,该方法限制了数据共享的灵活性和实时性,在实际中并不可行[6-7]。

为解决上述问题,Blaze 等人[8]提出了代理重加密(Proxy Encryption,PRE)的概念。在 PRE 中,当数据拥有者想要与某个授权用户共享数据时,其能够生成一个重加密密钥使得代理者将数据拥有者的密文转换为授权用户可解的密文,并且该转换过程不会泄漏数据和私钥信息。为解决证书管理问题,通过将标识加密(Identity-Based Encryption,IBE)和 PRE 结合,Green 等人[9]提出标识代理重加密(Identity-Based PRE,IBPRE)的概念,基于文献[10]构造了两个实用的 IBPRE 方案。然而,IBPRE 仅支持一对一数据共享,即数据拥有者一次只能为一个授权用户生成重加密密钥。当数据拥有者与一组授权用户共享数据时,其生成一组重加密密钥且代理者需要多次执行重加密操作,造成大量资源的浪费。

为满足多用户场景,Xu 等人[11]将广播加密的思想应用于 IBPRE 中提出标识广播代理重加密(Identity-Based Broadcast PRE,IBBPRE)。数据拥有者能够为一个授权用户集合生成重加密密钥,代理者使用该密钥能够将数据拥有者的密文转换为授权用户标识集合下的重加密密文。该密文只有属于授权用户集合的用户才能够解密成功获得数据,其他用户即使合谋也不会得到密文中的内容[12]。随

后，IBBPRE 得到了学术界的广泛关注和进一步发展，实现了可撤销[13]、条件[14]、匿名[15-16]、双向访问控制[17]等功能。

PRE 可用性建立在代理者诚实执行重加密操作基础上。然而，实际代理者极有可能为节约本地存储空间和计算资源而生成错误重加密密文。针对不可信代理者返回错误密文问题，Ohata 等人[18]引入了重加密可验证性概念，提出可验证代理重加密(Verifiable PRE，VPRE)方案实现重加密密文的正确性验证。然而，该方案验证阶段需要数据拥有者和授权用户联合验证，导致计算资源和通信资源的浪费。此外，其无法解决代理者在诚实转换密文时被恶意追责的情况。针对该问题，Ge 等人[19]在可验证性的基础上引入公平性概念，提出可验证公平属性基 PRE 方案。该方案利用承诺思想，通过消息锁加密技术在初始密文中对数据和随机数生成额外承诺，确保重加密可验证性和公平性。基于文献[19]的思想，Sun 等人[20]和 Jiang 等人[21]提出可验证公平 IBBPRE 方案。然而，在方案[19-21]重加密密文正确性验证中，需要传输原始密文和重加密密钥引发额外通信开销，且造成重加密密钥泄露；同时，如果代理者提供错误的原始密文和重加密密钥，导致方案不能满足可验证性；此外，密文生成阶段需生成额外承诺致使计算代价增加。

SM9[22]作为我国自主研发的标识密码算法，实现了国家核心技术自主可控的战略性需求。目前，SM9 系列算法已经成为国家标准和 ISO/IEC 国际标准，其在国内外的地位愈发重要。但是 SM9 标识加密算法仅考虑一对一应用场景，无法满足多用户场景中一对多数据共享需求。结合 SM9 算法和广播加密，基于 SM9 的广播加密[23-25]被提出。然而这些方案不支持密文转换，导致灵活性较差，阻遏国产密码算法的实际应用。尽管 Liu 等人[26]提出基于 SM9 的 IBPRE 方案，但其仅实现基础密文转换功能，未解决不可信代理者返回错误密文问题且不支持一对多数据共享。

为解决上述问题，本文提出基于 SM9 的可验证公平标识广播代理重加密方案，具体贡献如下：

(1)基于 SM9 标识加密算法，本文提出可验证公平标识广播代理重加密方案，实现了多用户场景中一对多的安全数据共享。所提方案采取与 SM9 加密算法一致的用户私钥提取算法，使其能够与现有 SM9 系统高效融合。此外，重加密密钥和重加密密文的长度保持恒定，与授权用户数量无关。

(2)借鉴 Fujisaki-Okamoto 转换[27]的思想，所提方案将数据融入随机数中无需生成额外承诺，实现重加密可验证性，即授权用户能够在解密时验证代理者是否诚实生成重加密密文。此外，通过设计高效零知识证明协议，所提方案能够满足公平性，即若代理者诚实转换密文则不会被恶意追责。

(3)本文优化可验证公平标识广播代理重加密的形式化定义和安全模型，其中验证阶段可公开执行，无需原始密文和重加密密钥参与，降低通信开销同时保证重加密密钥安全。基于(P,Q)-GDDHE 假设、q-SDH 假设、哈希函数抗碰撞假设和零知识证明可靠性，在随机预言机模型中，证明所提方案满足静态选择明文攻击下不可区分性、合谋攻击下抗密钥泄露性、可验证性和公平性。

(4)理论和实验分析表明，所提方案和已知方案相比取得了计算代价和存储代价方面优势。当授权用户数量为 20 时，所提方案生成重加密密钥需要 163.72 ms，比已有方案降低至少 59.51%；解密重加密密文需要 483.06 ms，比已有方案降低至少 22.27%。因此，所提方案更加适用于多用户数据共享场景。

2　相关工作

(1)标识代理重加密

1998 年，Blaze 等人[8]提出 PRE 的概念，实现密文数据安全共享。随后，学者们提出具备各种功能的 PRE 方案，包括条件[28]、可问责[29]、细粒度[30]等。然而，这些方案均存在着证书管理问题。因此，Green 等人[9]通过结合 IBE 和 PRE，提出 IBPRE。考虑到已有方案均假设数据拥有者和授权用户在同一个域中，Tang 等人[31]提出域间 IBPRE 方案以支持跨域密文转换。为实现重加密密文的重加密操作，Wang 等人[32]提出多跳 IBPRE 方案。不幸的是，上述方案[9,31-32]均不能抵抗合谋攻击，即一旦代理者和授权用户合谋，数据拥有者的私钥就会泄漏。为解决该问题，Wang 等人[33]提出抗合谋 IBPRE 方案。然而，该方案中数据拥有者无法自主生成重加密密钥，依赖于 PKG 辅助及安全信道，导致 PKG 须长期在线，降低系统实用性。Liang 等人[34]在标准模型中构造抗合谋条件 IBPRE 方案，其中密文和重加密密钥均被嵌入条件，只有当两者条件一致时，才能够进行重加密操作，实现细粒度共享。然而，上述方案均假设代理者诚实转换密文，而现实中代理

者可能为最大化自身利益，返回错误密文给授权用户。针对该问题，Ohata 等人[18]提出 VPRE 方案。随后，Lin 等人[35]提出支持委托验证的 PRE，引入验证者使用数据拥有者颁发的验证密钥对重加密密文进行验证。Zhan 等人[36]扩展了重加密可验证方式，支持公开、私有以及委托验证。然而，上述方案仅满足一对一共享需求，在多用户数据共享场景中灵活性差。

(2)标识广播代理重加密

为提高多用户场景下共享效率，Xu 等人[11]提出 IBBPRE 概念，使得代理者能够将原始密文转换为多个授权用户可解的广播密文，极大降低数据拥有者和代理者的开销。针对授权用户撤销问题，Ge 等人[13]提出一个可撤销的 IBBPRE 方案，其中代理者能够撤销重加密密钥中授权用户的解密能力。考虑到 IBBPRE 中授权用户解密重加密密文时需了解其他授权用户身份，Maiti 等人[15]提出隐私保护的 IBBPRE 方案，采用拉格朗日插值方法生成重加密密钥保护授权用户身份隐私。然而，该方案中重加密密钥和密文长度随授权用户数量增加，因此，Zhang 等人[16]提出基于假名的 IBBPRE 方案，其解密算法开销恒定。结合匹配加密，Sun 等人[17]提出支持双向访问控制的 IBBPRE 方案，确保密文真实性。Ge 等人[19]利用消息锁加密技术生成额外承诺，提出可验证公平属性基 PRE，实现细粒度数据共享的同时满足代理者行为可验证。扩展该思想至 IBBPRE 中，Sun 等人[20]和 Jiang 等人[21]提出可验证公平 IBBPRE 方案。然而，上述方案存在着计算代价和通信开销过大及未考虑代理提供错误信息导致验证失败问题。

(3) SM9

2016 年，国家密码管理局提出 SM9 系列算法[22]，包括数字签名、密钥交换、密钥封装和公钥加密。之后，学者们针对 SM9 算法进行广泛的拓展研究。Cheng 等人[37]形式化证明密钥封装和公钥加密的安全性。Lai 等人[38]基于更弱的假设优化了密钥封装算法并证明了数字签名算法的安全性。为提高 SM9 算法效率，Zhen 等人[39]优化了双线性映射的 Miller loop 过程；Hu 等人[40]提出了 SM9 算法中 R-ate 对的快速计算方法。为拓展 SM9 功能，标识广播加密[23-25]、IBPRE[26]、属性基签名[41]、环签名[42-43]、仲裁 IBE[44]、分层 IBE[45-46]、签密[47]、支持等性测试的抗渗透标识加密[48]等多功能方案被提出。综上，目前未见有关基于 SM9 的标识广播代理重加密研究。

3 预备知识

3.1 双线性映射

令 $\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_T$ 为素数 N 阶的乘法循环群，双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$ 满足如下性质[10]：

(1)双线性。对于任意的 $g\in\mathbb{G}_1$，$h\in\mathbb{G}_2$，$a,b\in\mathbb{Z}_N^*$，有 $e(g^a,h^b)=e(g,h)^{ab}$。

(2)非退化性。存在 $g\in\mathbb{G}_1$，$h\in\mathbb{G}_2$，使得 $e(g,h)\neq1$。

(3)可计算性。对于任意的 $g\in\mathbb{G}_1$，$h\in\mathbb{G}_2$，$e(g,h)$ 可被高效计算。

若 $\mathbb{G}_1=\mathbb{G}_2$，则 e 是一个对称双线性映射(类型 I 映射)；否则为非对称双线性映射(类型 II 和 III 映射)。在类型 II 映射中，存在一个公开可计算的同构 $\varphi:\mathbb{G}_2\rightarrow\mathbb{G}_1$。SM9 算法基于类型 II 映射构造。

3.2 零知识证明

零知识证明[49]是一种证明系统。令 $\mathcal{R}=\{(x,w):\{0,1\}^*\times\{0,1\}^*\}$ 为可计算二元关系，其中 x 是陈述，w 是证据。设 $\mathcal{L}(\mathcal{R})$ 为 $\mathcal{R}$ 中有效陈述组成的 NP 语言。证明者能够在不泄漏 w 的情况下，使验证者相信其拥有 w 且 $(x,w)\in\mathcal{R}$。定义 $\Pi=ZKPoK\{(w):x=g^w\}$ 为证明离散对数关系的零知识证明系统。通过 Fiat-Shamir 转换，可以在随机预言机模型中将交互式零知识证明系统转换为非交互式零知识证明系统，其包含以下 2 个多项式时间算法：

(1)$\pi\leftarrow\mathrm{Prove}(w,x)$。输入证据 w 和陈述 x，输出证明 π。

(2)$\{1/0\}\leftarrow\mathrm{Verify}(x,\pi)$。输入陈述 x 和证明 π，若证明有效，输出 1；否则输出 0。

非交互式零知识证明系统需满足完备性、可靠性和零知识性。

完备性：对于任意 $(x,w)\in\mathcal{R}$，诚实证明者生成的证明 π 被验证者接受的概率为 1。

可靠性：对于任意 $w^*\notin\mathcal{L}(\mathcal{R})$，恶意证明者生成的证明 π^* 被验证者接受的概率可忽略。

零知识性：对于任意 $(x,w)\in\mathcal{R}$，存在概率多项式时间(Probabilistic Polynomial Time，PPT)算法 $\mathcal{S}$，其生成的证明 π^* 与证明者生成的证明 π 不可区分。

3.3 困难问题假设

本文所提方案的安全性基于 (P,Q)-GDDHE 假设[23]、q-SDH 假设[50]和哈希函数抗碰撞假设[51]。

(P,Q)-GDDHE 问题：给定 $\{g_0, g_0^a, g_0^{a^2}, \cdots, g_0^{a^{2n}}, g_0^{\nu P(a)}, h_0^a, h_0^{a^2}, \cdots, h_0^{a^k}, h_0^{a^2Q(a)}, h_0^{\nu a^2 Q(a)}, Z\}$，判断 $Z = e(g_0,h_0)^{\nu a Q(a)}$ 是否成立，其中 $P(x)=\prod_{i=k+1}^{k+n}(x+\kappa_i)$ 和 $Q(x)=\prod_{i=1}^{k}(x+\kappa_i)$ 是两个互质多项式，$g_0\in\mathbb{G}_1$，$h_0\in\mathbb{G}_2$，$Z\in\mathbb{G}_T$，$\kappa_1,\cdots,\kappa_{n+k}\in\mathbb{Z}_N^*$，且 $\nu,a\in\mathbb{Z}_N^*$ 未知。

(P,Q)-GDDHE 假设：任何 PPT 算法 $\mathcal{A}$ 解 (P,Q)-GDDHE 问题的优势 $Adv=|\Pr[\mathcal{A}(g_0, g_0^a, g_0^{a^2}, \cdots, g_0^{a^{2n}}, g_0^{\nu P(a)}, h_0^a, h_0^{a^2}, \cdots, h_0^{a^k}, h_0^{a^2Q(a)}, h_0^{\nu a^2Q(a)}, Z = e(g_0,h_0)^{\nu a Q(a)})=1]-\Pr[\mathcal{A}(g_0, g_0^a, g_0^{a^2}, \cdots, g_0^{a^{2n}}, g_0^{\nu P(a)}, h_0^a, h_0^{a^2}, \cdots, h_0^{a^k}, h_0^{a^2Q(a)}, h_0^{\nu a^2Q(a)}, Z\neq e(g_0, h_0)^{\nu a Q(a)})=1]|$ 是可忽略的。

q-SDH 问题：给定 $\{g_0,h_0,h_0^a,h_0^{a^2},\cdots,h_0^{a^q}\}$，寻找 $\{\nu, g_0^{1/(a+\nu)}\}$，其中 $g_0\in\mathbb{G}_1$，$h_0\in\mathbb{G}_2$，$\nu\in\mathbb{Z}_N^*$，且 $a\in\mathbb{Z}_N^*$ 未知。

q-SDH 假设：任何 PPT 算法 $\mathcal{A}$ 解 q-SDH 问题的优势 $Adv=|\Pr[\mathcal{A}(g_0,h_0,h_0^a,h_0^{a^2},\cdots,h_0^{a^q})=\{\nu,g_0^{1/(a+\nu)}\}]|$ 是可忽略的。

哈希函数抗碰撞问题：给定密码哈希函数 $\mathcal{H}:\{0,1\}^{\lambda_1}\to\{0,1\}^{\lambda_2}$，寻找 $\{m,m'\}$ 满足 $m\neq m'$ 且 $\mathcal{H}(m)=\mathcal{H}(m')$，其中 λ_1 和 λ_2 分别是输入和输出长度。

哈希函数抗碰撞假设：任何 PPT 算法 $\mathcal{A}$ 解哈希函数抗碰撞问题的概率 $Adv=\Pr[\mathcal{A}(\mathcal{H})=\{m,m'\}: m\neq m'\wedge\mathcal{H}(m)=\mathcal{H}(m')]$ 是可忽略的。

4　可验证公平标识广播代理重加密

4.1　系统模型

可验证公平标识广播代理重加密的系统模型（见图 1）由五类实体组成：密钥生成中心（Private Key Generator，PKG）、云服务器（Cloud Server，CS）、数据拥有者（Data Owner，DO）和授权用户（Authorized Users，AU）。PKG 负责建立整个系统生成系统参数和主私钥，以及为系统中的用户生成用户私钥。CS 负责存储和转换初始密文为重加密密文。DO 能够生成初始密文并将其外包给 CS 进行存储，从 CS 处下载初始密文并解密得到消息，以及为一组 AU 生成重加密密钥以共享密文数据。AU 从 CS 处下载重加密密文并解密验证得到消息。如果 CS 返回错误重加密密文，AU 能够生成错误报告以证明云服务器存在非法行为。此外，任何人都能够依据该报告检查 CS 是否诚实执行重加密操作。

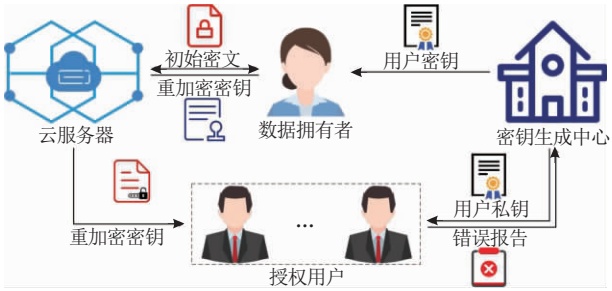

图 1　系统模型

4.2　形式化定义

定义 1.　可验证公平标识广播代理重加密由 8 个多项式时间算法组成。

(1) Setup(λ,n)：该算法由 PKG 执行。输入安全参数 λ 和授权用户最大数量 n，PKG 生成系统参数 $params$ 和主私钥 msk。

(2) Extract(msk,id_u)：该算法由 PKG 执行。输入主私钥 msk 和用户标识 id_u，PKG 生成用户私钥 SK_{id_u}。

(3) Encrypt(id_o,m)：该算法由 DO 执行。输入用户标识 id_o 和消息 m，DO 输出初始密文 C。

(4) Re-KeyGen(SK_{id_o},S)：该算法由 DO 执行。输入用户私钥 SK_{id_o} 和授权用户标识集合 S，DO 输出重加密密钥 $rk_{id_o\to S}$。

(5) Re-Encrypt$(rk_{id_o\to S},C)$：该算法由 CS 执行。输入重加密密钥 $rk_{id_o\to S}$ 和初始密文 C，CS 输出重加密密文 C'。

(6) Decrypt(SK_{id_o},C)：该算法由 DO 执行。输入用户私钥 SK_{id_o} 和初始密文 C，DO 输出消息 m。

(7) DecVerify(SK_{id_j},C',S)：该算法由 AU_j 执行。输入用户私钥 SK_{id_j}、重加密密文 C' 和用户标识集合 S 满足 $id_j\in S$ 且 $|S|\leq n$，若 C' 是有效的重加密密文，AU_j 输出消息 m；否则输出错误报告 π。

(8) Claim(id_j,C',π,S)：该算法由公开验证者执行。输入用户标识 id_j、重加密密文 C'、错误报告 π 和用户标识集合 S 满足 $id_j\in S$，若 C' 是错误的重加密密文，公开验证者输出 1；否则输出 0。

正确性：对任意的用户标识 id_o，集合 S，标识 $id_j\in S$，消息 m，$\{params,msk\}\leftarrow$Setup(λ,n)，$C\leftarrow$Encrypt(id_o,m)，$SK_{id_o}\leftarrow$Extract(msk,id_o)，$SK_{id_j}\leftarrow$Extract(msk,id_j)，$rk_{id_o\to S}\leftarrow$Re-KeyGen(SK_{id_o},S) 和 $C'\leftarrow$Re-Encrypt$(rk_{id_o\to S},C)$，有 $m\leftarrow$Decrypt(SK_{id_o},C) 和 $m\leftarrow$DecVerify(SK_{id_j},C',S)。

4.3　威胁模型

在可验证公平标识广播代理重加密中，PKG 和

DO 是完全可信的。具体地,PKG 诚实地建立系统,为用户分发私钥;DO 按照协议加密自己的消息并与 AU 进行分享。CS 和 AU 是不可信实体。一方面,CS 可能为节约本地存储空间和计算资源而产生错误重加密密文发送给 AU;另一方面,AU 可能会对诚实执行协议的 CS 恶意指控。同时,CS 可能与部分 AU 进行合谋,试图推断 DO 的私钥。

4.4 安全模型

可验证公平标识广播代理重加密应该满足静态选择明文攻击下的不可区分性(Indistinguishability against selective Identity and Chosen Plaintext Attack,IND-sID-CPA)、合谋攻击下的私钥抗泄露性(Secret Key Leakage Resistance against Collusion Attack,SKLR-CA)、可验证性(Verifiability)和公平性(Fairness)。安全模型由挑战者和攻击者$\mathcal{A}$之间的交互游戏定义。

IND-sID-CPA-I 游戏:

初始化:$\mathcal{A}$输出挑战标识 id^*。

系统建立:$\mathcal{C}$运行 Setup 算法生成系统参数 $params$ 和主私钥 msk,将 $params$ 发送给$\mathcal{A}$。

询问 1:$\mathcal{A}$能够适应性地进行以下询问:

(1)私钥提取询问:输入用户标识 id_i 满足 $id_i \neq id^*$,$\mathcal{C}$运行 Extract 算法生成用户私钥 SK_{id_i} 并返回给$\mathcal{A}$。

(2)重加密密钥提取询问:输入用户标识 id_i 和授权用户标识集合 S_i 满足 $id_i \neq id^*$,$\mathcal{C}$运行 Re-KeyGen 算法生成重加密密钥 $rk_{id_i \to S_i}$ 并返回给$\mathcal{A}$。

挑战:$\mathcal{A}$输出两个消息(m_0^*, m_1^*),$\mathcal{C}$随机选择一个比特 $b \in \{0,1\}$,运行 Encrypt 算法生成挑战密文 C_b^* 并返回给$\mathcal{A}$。

询问 2:$\mathcal{A}$继续进行询问 1 中的询问。

猜测:$\mathcal{A}$输出猜测 b'。若 $b'=b$,则$\mathcal{A}$赢得游戏。

$\mathcal{A}$赢得 IND-sID-CPA-I 游戏的优势定义为

$$Adv_{\mathcal{A}}^{\text{CPA-I}} = \left| \Pr[b'=b] - \frac{1}{2} \right| 。$$

IND-sID-CPA-II 游戏:

初始化:$\mathcal{A}$输出挑战标识集合 S^*。

系统建立:与 IND-sID-CPA-I 游戏相同。

询问 1:$\mathcal{A}$能够适应性地进行以下询问:

(1)私钥提取询问:输入用户标识 id_i 满足 $id_i \notin S^*$,$\mathcal{C}$运行 Extract 算法生成用户私钥 SK_{id_i} 并返回给$\mathcal{A}$。

(2)重加密密钥提取询问:输入用户标识 id_i 和授权用户标识集合 S_i 满足 $id_i \notin S^*$,$\mathcal{C}$运行 Re-KeyGen 算法生成重加密密钥 $rk_{id_i \to S_i}$ 并返回给$\mathcal{A}$。

挑战:$\mathcal{A}$输出两个消息(m_0^*, m_1^*)和用户标识 id 作为挑战,$\mathcal{C}$随机选择一个比特 $b \in \{0,1\}$,运行 Re-Encrypt 算法生成挑战密文 $C_b'^*$ 并返回给$\mathcal{A}$。

询问 2:与 IND-sID-CPA-I 游戏相同。

猜测:与 IND-sID-CPA-I 游戏相同。

$\mathcal{A}$赢得 IND-sID-CPA-II 游戏的优势定义为

$$Adv_{\mathcal{A}}^{\text{CPA-II}} = \left| \Pr[b'=b] - \frac{1}{2} \right| 。$$

定义 1. 如果任何多项式时间攻击者$\mathcal{A}$的优势 $Adv_{\mathcal{A}}^{\text{CPA-I}}$ 和 $Adv_{\mathcal{A}}^{\text{CPA-II}}$ 是可忽略的,则可验证公平标识广播代理重加密方案是 IND-sID-CPA 安全的。

SKLR-CA 游戏:

初始化:与 IND-sID-CPA-I 游戏相同。

系统建立:与 IND-sID-CPA-I 游戏相同。

询问 1:$\mathcal{A}$能够适应性地进行以下询问:

(1)私钥提取询问:输入用户标识 id_i 满足 $id_i \neq id^*$,$\mathcal{C}$运行 Extract 算法生成用户私钥 SK_{id_i} 并返回给$\mathcal{A}$。

(2)重加密密钥提取询问:输入用户标识 id_i 和授权用户标识集合 S_i,$\mathcal{C}$运行 Re-KeyGen 算法生成重加密密钥 $rk_{id_i \to S_i}$ 并返回给$\mathcal{A}$。

输出:$\mathcal{A}$输出 id^* 的私钥 SK^*。如果 SK^* 是 id^* 的有效私钥,则$\mathcal{A}$赢得游戏。

$\mathcal{A}$赢得游戏 SKLR-CA 的优势定义为

$$Adv_{\mathcal{A}}^{\text{CA}} = |\Pr[SK^* = SK_{id^*}]| 。$$

定义 2. 如果任何多项式时间攻击者$\mathcal{A}$的优势 $Adv_{\mathcal{A}}^{\text{CA}}$ 是可忽略的,则可验证公平标识广播代理重加密方案是 SKLR-CA 安全的。

Verifiability 游戏:

系统建立:与 IND-sID-CPA-I 游戏相同。

询问 1:$\mathcal{A}$能够适应性地进行以下询问:

(1)私钥提取询问:输入用户标识 id_i,$\mathcal{C}$运行 Extract 算法生成用户私钥 SK_{id_i} 并返回给$\mathcal{A}$。

(2)重加密密钥提取询问:与 SKLR-CA 游戏相同。

挑战:$\mathcal{A}$输出消息 m^*,用户标识 id^* 和授权用户标识集合 S^* 作为挑战,$\mathcal{C}$运行 Encrypt 和 Re-KeyGen 算法生成挑战密文 C^* 和重加密密钥 $rk_{id^* \to S^*}$ 并返回给$\mathcal{A}$。

输出:$\mathcal{A}$输出重加密密文 C'^*。$\mathcal{C}$随机选择 $id \in$

S^*，运行 Extract 算法生成用户私钥 SK_{id}，运行 DecVerify 算法得到解密结果 m'^*，如果 $m'^* \neq m^*$，则 $\mathcal{A}$ 赢得游戏。

$\mathcal{A}$ 赢得 Verifiability 游戏的优势定义为

$$Adv_{\mathcal{A}}^{\mathrm{Ver}} = |\Pr[m'^* \neq m^*]|。$$

定义 3.　如果任何多项式时间攻击者 $\mathcal{A}$ 的优势 $Adv_{\mathcal{A}}^{\mathrm{Ver}}$ 是可忽略的，则可验证公平标识广播代理重加密方案满足可验证性。

Fairness 游戏：

系统建立：与 IND-sID-CPA-I 游戏相同。

询问 1：与 Verifiability 游戏相同。

挑战 1：$\mathcal{A}$ 输出消息 m^*，用户标识 id 和授权用户标识集合 S^* 作为挑战，$\mathcal{C}$ 运行 Re-Encrypt 算法生成挑战密文 C'^* 并返回给 $\mathcal{A}$。

输出：$\mathcal{A}$ 输出错误报告 π^* 和授权用户标识 id^* 满足 $id^* \in S^*$。如果 $\mathrm{Claim}(id^*, C'^*, \pi^*, S^*)=1$，则 $\mathcal{A}$ 赢得游戏。

$\mathcal{A}$ 赢得 Fairness 游戏的优势定义为

$$Adv_{\mathcal{A}}^{\mathrm{Fair}} = |\Pr[\mathrm{Claim}(id^*, C'^*, \pi^*, S^*)=1]|。$$

定义 4.　如果任何多项式时间攻击者 $\mathcal{A}$ 的优势 $Adv_{\mathcal{A}}^{\mathrm{Fair}}$ 是可忽略的，则可验证公平标识广播代理重加密方案满足公平性。

5　方案构造

本节给出了基于 SM9 的可验证公平标识广播代理重加密的具体构造。表 1 列出本文方案涉及的符号定义。

表 1　符号定义

符号	定义
$params$	系统参数
(id_o, SK_{id_o})	数据拥有者的用户标识和私钥
S	授权用户标识集合
(id_j, SK_{id_j})	第 j 个授权用户的用户标识和私钥
$rk_{id_o \to S}$	重加密密钥
C	初始密文
C'	重加密密文
π	错误报告

5.1　方　案

(1) Setup：给定安全参数 λ 和授权用户最大数量 n，PKG 执行：

① 生成双线性映射 $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$，其中 $\mathbb{G}_1$、$\mathbb{G}_2$ 和 $\mathbb{G}_T$ 均是素数 N 阶乘法循环群，g 和 h 分别为 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元。

② 随机选择 $\alpha \in \mathbb{Z}_N^*$，$u \in \mathbb{G}_2$，计算 $\sigma = e(g,h)^{\alpha}$，$h_2 = h^{\alpha^2}$，设定主私钥 $msk = \{\alpha, h\}$。

③ 随机选择密钥生成函数标识 hid，选定密码哈希函数 $H, H_1, H_2, H_3: \{0,1\}^* \to \mathbb{Z}_N^*$，密钥派生函数 $KDF: \{0,1\}^* \to \{0,1\}^l$，其中 l 为消息的长度。

④ 输出系统参数 $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N, n, g, u, h_2, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^n}, \sigma, hid, H, H_1, H_2, H_3, KDF\}$。

(2) Extract：给定用户标识 $id_u \in \{0,1\}^*$，PKG 计算并输出用户私钥 $SK_{id_u} = h^{\alpha/(\alpha + H(id_u \| hid, N))}$。

(3) Encrypt：给定用户标识 $id_o \in \{0,1\}^*$ 和消息 m，DO 执行：

① 随机选取 $\chi \in \mathbb{G}_T$。

② 计算 $r = H_1(m \| \chi, N)$，$c_0 = \sigma^r \cdot \chi$，$c_1 = g^{r \cdot (\alpha + H(id_o \| hid, N))}$，$c_2 = u^r$，$c_3 = m \oplus KDF(\chi)$。

③ 输出初始密文 $C = \{c_0, c_1, c_2, c_3\}$。

(4) Re-KeyGen：给定授权用户标识集合 $S = \{id_1, \cdots, id_\eta\}$ $(\eta < n)$，DO 执行：

① 随机选取 $t_1, t_2 \in \mathbb{Z}_N^*$，计算 $T = \sigma^{t_1}$，$k = H_2(T)$。

② 计算 $rk_0 = SK_{id_o} \cdot u^{t_2 \cdot k}$，$rk_1 = g^{t_2 \cdot (\alpha + H(id_o \| hid, N))}$，$rk_2 = g^{t_1 \cdot \prod_{l=1}^{\eta} (\alpha + H(id_l \| hid, N))}$，$rk_3 = h_2^{t_1}$。

③ 输出重加密密钥 $rk_{id_o \to S} = \{rk_0, rk_1, rk_2, rk_3\}$。

(5) Re-Encrypt：给定重加密密钥 $rk_{id_o \to S} = \{rk_0, rk_1, rk_2, rk_3\}$ 和初始密文 $C = \{c_0, c_1, c_2, c_3\}$，CS 执行：

① 计算 $c_0' = c_0 \cdot e(c_1, rk_0)^{-1}$，$c_1' = rk_1$，$c_2' = c_2$，$c_3' = rk_2$，$c_4' = c_3$，$c_5' = rk_3$。

② 输出重加密密文 $C' = \{c_0', c_1', c_2', c_3', c_4'\}$。

(6) Decrypt：给定初始密文 $C = \{c_0, c_1, c_2, c_3\}$，DO 计算 $\chi' = c_0 \cdot e(c_1, SK_{id_o})^{-1}$，$m' = KDF(\chi') \oplus c_3$，输出消息 m'。

(7) DecVerify：给定重加密密文 $C' = \{c_0', c_1', c_2', c_3', c_4'\}$ 和用户标识集合 $S = \{id_1, \cdots, id_\eta\}$，用户标识为 $id_j \in S$ 的 AU_j 执行：

① 记 $\Delta_1 = \prod_{l=1, l \neq j}^{\eta} H(id_l \| hid, N)$，$\Delta_2 = \left(\Delta_1 - \prod_{l=1, l \neq j}^{\eta} (\alpha + H(id_l \| hid, N))\right) \Big/ \alpha$。

② 计算 $T' = (e(c_3', SK_{id_j}) \cdot e(g^{\Delta_2}, c_5'))^{1/\Delta_1}$。

③ 计算 $k' = H_2(T')$，$\chi' = c_0' \cdot e(c_1'^{k'}, c_2')$，$m' = KDF(\chi') \oplus c_4'$。

④ 计算 $r' = H_1(m' \| \chi', N)$，判断 $c_2' = u^{r'}$ 是否

成立，如果成立，输出消息 m'；否则执行⑤。

⑤ 调用 ZKPOK 协议 $\Pi=ZKPoK\{(SK_{id_j}):\sigma=e(g^{\alpha+H(id_j\|hid,N)},SK_{id_j})\wedge T'=(e(c_3',SK_{id_j})\cdot e(g^{\Delta_2},c_5'))^{1/\Delta_1}\}$ 生成错误报告，具体如下：

(a) 随机选择 $R\in\mathbb{G}_2$。

(b) 计算 $T_1=e(g^{\alpha+H(id_j\|hid,N)},R)$，$T_2=e(c_3',R)^{1/\Delta_1}$。

(c) 计算 $c=H_3(id_j,T',C',S,T_1,T_2)$。

(d) 计算 $res=R\cdot SK_{id_j}^c$。

(e) 输出错误报告 $\pi=\{T',c,res\}$。

(8) Claim：输入用户标识 id_j，重加密密文 $C'=\{c_0',c_1',c_2',c_3',c_4'\}$，错误报告 $\pi=\{T',c,res\}$ 和用户标识集合 $S=\{id_1,\cdots,id_\eta\}$ 满足 $id_j\in S$，公开验证者执行：

① 调用 ZKPOK 协议 Π，验证错误报告的有效性，具体如下：

(a) 计算 $T_1'=e(g^{\alpha+H(id_j\|hid,N)},res)\cdot\sigma^{-c}$，$T_2'=e(c_3',res)^{1/\Delta_1}\cdot(T'\cdot e(g^{\Delta_2},c_5')^{-1/\Delta_1})^{-c}$。

(b) 计算 $c'=H_3(id_j,T',C',S,T_1',T_2')$。

(c) 判断 $c'=c$ 是否成立，如果成立，则执行②；否则，输出 0，表明错误报告无效。

② 计算 $k'=H_2(T')$，$\chi'=c_0'\cdot e(c_1'^{k'},c_2')$，$m'=KDF(\chi')\oplus c_4'$。

③ 计算 $r'=H_1(m'\|\chi',N)$，判断 $c_2'\neq u^{r'}$ 是否成立。如果成立，则输出 1，表明 C' 是错误的重加密密文即 CS 未诚实转换密文；否则输出 0。

5.2 正确性

(1) 对于 Decrypt 算法，有

$$\begin{aligned}\chi'&=c_0\cdot e(c_1,SK_{id_o})^{-1}\\&=\sigma^r\cdot\chi\cdot e(g^{r\cdot(\alpha+H(id_o\|hid,N))},h^{\alpha/(\alpha+H(id_o\|hid,N))})^{-1}\\&=\sigma^r\cdot\chi\cdot e(g^r,h^\alpha)^{-1}=\chi,\\m'&=KDF(\chi')\oplus c_3\\&=KDF(\chi')\oplus m\oplus KDF(\chi)=m。\end{aligned}$$

(2) 对于 DecVerify 算法，有

$$\begin{aligned}T'&=(e(c_3',SK_{id_j})\cdot e(g^{\Delta_2},c_5'))^{1/\Delta_1}\\&=(e(g^{t_1\cdot\prod_{l=1}^{\eta}(\alpha+H(id_l\|hid,N))},h^{\alpha/(\alpha+H(id_j\|hid,N))})\cdot\\&\quad e(g^{\Delta_2},h_2^{t_1}))^{1/\Delta_1}\\&=(e(g,h)^{t_1\alpha\cdot\prod_{l=1,l\neq j}^{\eta}(\alpha+H(id_l\|hid,N))}\cdot e(g,h)^{t_1\alpha^2\cdot\Delta_2})^{1/\Delta_1}\\&=(e(g,h)^{t_1\alpha\cdot(\Delta_1-\alpha\cdot\Delta_2)}\cdot e(g,h)^{t_1\alpha^2\cdot\Delta_2})^{1/\Delta_1}\\&=e(g,h)^{t_1\alpha}=\sigma^{t_1}=T,\\k'&=H_2(T')=H_2(T)=k,\\\chi'&=c_0'\cdot e(c_1'^{k'},c_2')\\&=\chi\cdot e(g^{r\cdot(\alpha+H(id_o\|hid,N))},u^{t_2\cdot k})^{-1}\cdot\\&\quad e(g^{k'\cdot t_2\cdot(\alpha+H(id_o\|hid,N))},u^r)\\&=\chi,\\m'&=KDF(\chi')\oplus c_4'=KDF(\chi')\oplus m\oplus KDF(\chi)=m。\end{aligned}$$

(3) 对于 Claim 算法，有

$$\begin{aligned}T_1'&=e(g^{\alpha+H(id_j\|hid,N)},res)\cdot\sigma^{-c}\\&=e(g^{\alpha+H(id_j\|hid,N)},R\cdot SK_{id_j}^c)\cdot\sigma^{-c}\\&=e(g^{\alpha+H(id_j\|hid,N)},R)=T_1,\\T_2'&=e(c_3',res)^{1/\Delta_1}\cdot(T'\cdot e(g^{\Delta_2},c_5')^{-1/\Delta_1})^{-c}\\&=e(c_3',R\cdot SK_{id_j}^c)^{1/\Delta_1}\cdot((e(c_3',SK_{id_j})\cdot\\&\quad e(g^{\Delta_2},c_5'))^{1/\Delta_1}\cdot e(g^{\Delta_2},c_5')^{-1/\Delta_1})^{-c}\\&=e(c_3',R)^{1/\Delta_1}=T_2。\end{aligned}$$

5.3 安全性

定理 1. 所提方案中的 ZKPOK 协议 Π 在随机预言机模型下是一个非交互式零知识证明系统。

证明. 协议 Π 的完备性、可靠性和零知识性证明如下：

完备性. 协议 Π 的完备性可通过 Claim 算法的正确性分析推导(见 5.2 节)。

可靠性. 利用知识证明系统的可提取性可以证明协议 Π 的可靠性。即若存在恶意证明者能够以不可忽略的优势 ξ 让验证者接受证明 π^*，那么我们可构造一个知识提取器 $\mathcal{E}$ 以不可忽略的优势输出知识 SK_{id_j}。具体地，假定攻击者 $\mathcal{A}$ 能够生成一个有效副本 $\{T',c,res\}$，其中 $c=H_3(id_j,T',C',S,T_1,T_2)$，那么 $\mathcal{E}$ 可通过倒带 $\mathcal{A}$ 至预言机询问 $H_3(id_j,T',C',S,T_1,T_2)$ 之前，设置哈希预言机使其满足 $c^*=H_3(id_j,T',C',S,T_1,T_2)\neq c$，进而获得另一有效副本 $\{T',c^*,res^*\}$。那么，$\mathcal{E}$ 可计算 $SK_{id_j}=(res^*/res)^{c^*-c}$ 提取知识。

零知识性. 基于 Fiat-Shamir 转换，我们可构造模拟器 $\mathcal{S}$ 以模拟与任意验证者的交互。具体地，给定一个要证明的陈述 $\{T'\}$，$\mathcal{S}$ 随机选择 $res^*\in\mathbb{G}_2$，$c^*\in\mathbb{Z}_N^*$，计算 $T_1^*=e(g^{\alpha+H(id_j\|hid,N)},res^*)\cdot\sigma^{-c^*}$，$T_2^*=e(c_3',res^*)^{1/\Delta_1}\cdot(T'\cdot e(g^{\Delta_2},c_5')^{-1/\Delta_1})^{-c^*}$，并设置哈希预言机使其满足 $c^*=H_3(id_j,T',C',S,T_1^*,T_2^*)$。最后，$\mathcal{S}$ 输出副本 $\{T',c^*,res^*\}$。可以观察到，由于 H_3 被模拟为一个随机预言机，任意验证者将会接受该副本。此外，res^* 和 c^* 的分布与真实协议中分布相同且 $\mathcal{S}$ 不掌握任何证据信息。因此，协议 Π 满足零知识性。 证毕。

定理 2.　如果(P,Q)-GDDHE 假设成立，则所提方案在随机预言机模型下是 IND-sID-CPA 安全的。

证明.　该定理由引理 1 和引理 2 证明。

引理 1.　假定攻击者$\mathcal{A}$能够以不可忽略的优势ξ赢得游戏 IND-sID-CPA-I，则存在算法$\mathcal{B}$能够以不可忽略的优势ξ'解(P,Q)-GDDHE 问题。

证明. 给定(P,Q)-GDDHE 实例$\{g_0,g_0^a,g_0^{a^2},\cdots,g_0^{a^{2n}},g_0^{\nu P(a)},h_0^a,h_0^{a^2},\cdots,h_0^{a^k},h_0^{a^2Q(a)},h_0^{\nu a^2Q(a)},Z\}$，$\mathcal{B}$的目标是判断$Z=e(g_0,h_0)^{\nu aQ(a)}$是否成立，其中$P(x)=\prod_{i=k+1}^{k+n}(x+\kappa_i)$和$Q(x)=\prod_{i=1}^{k}(x+\kappa_i)$是两个互质多项式，$\kappa_1,\cdots,\kappa_{n+k}\in\mathbb{Z}_N^*$。

初始化：$\mathcal{A}$输出挑战标识id^*。

系统建立：$\mathcal{B}$隐式设置$\alpha=a,h=h_0^{Q(a)}$，随机选择$\omega\in\mathbb{Z}_N^*$，计算$g=g_0^{\prod_{i=k+2}^{k+n}(a+\kappa_i)}$，$u=h_0^{\omega\cdot a^2Q(a)}$，$h_2=h_0^{a^2Q(a)}$，$g^a=g_0^{a\prod_{i=k+2}^{k+n}(a+\kappa_i)}$，$g^{a^2}=g_0^{a^2\prod_{i=k+2}^{k+n}(a+\kappa_i)}$，$\cdots$，$g^{a^n}=g_0^{a^n\prod_{i=k+2}^{k+n}(a+\kappa_i)}$，$\sigma=e(g_0^{\prod_{i=1}^{k}(a+\kappa_i)\cdot\prod_{i=k+2}^{k+n}(a+\kappa_i)},h_0^a)$。$\mathcal{B}$选择密钥生成函数标识$hid$，密钥派生函数$KDF:\{0,1\}^*\to\{0,1\}^l$，返回系统参数$params$给$\mathcal{A}$。

询问 1：$\mathcal{A}$能够适应性地进行以下询问：

(1) H 询问：$\mathcal{B}$维护初始为空的由元组(id_i,κ_i)组成的列表L。当$\mathcal{A}$对id_i进行H询问时，如果(id_i,κ_i)存在于L，$\mathcal{B}$返回κ_i给$\mathcal{A}$；否则，$\mathcal{B}$执行：

① 如果$id_i=id^*$，$\mathcal{B}$插入(id_i,κ_{k+1})到L中，并返回κ_{k+1}给$\mathcal{A}$。

② 如果$id_i\neq id^*$，$\mathcal{B}$随机选择$\kappa_i\in[\kappa_1,\kappa_k]$，插入$(id_i,\kappa_i)$到$L$中，并返回$\kappa_i$给$\mathcal{A}$。

(2) H_1询问：$\mathcal{B}$维护初始为空的由元组(m_i,χ_i,ζ_i)组成的列表L_1。当$\mathcal{A}$对(m_i,χ_i)进行H_1询问时，如果(m_i,χ_i,ζ_i)存在于L_1，$\mathcal{B}$返回ζ_i给$\mathcal{A}$；否则，$\mathcal{B}$随机选择$\zeta_i\in\mathbb{Z}_N^*$，插入(m_i,χ_i,ζ_i)到L_1中，并返回ζ_i给$\mathcal{A}$。

(3) H_2询问：$\mathcal{B}$维护初始为空的由元组(T_i,τ_i)组成的列表L_2。当$\mathcal{A}$对T_i进行H_2询问时，如果(T_i,τ_i)存在于L_2，$\mathcal{B}$返回τ_i给$\mathcal{A}$；否则，$\mathcal{B}$随机选择$\tau_i\in\mathbb{Z}_N^*$，插入(T_i,τ_i)到L_2中，并返回τ_i给$\mathcal{A}$。

(4) H_3询问：$\mathcal{B}$维护初始为空的由元组$(id_i,T_i,C_i',S_i,T_{1,i},T_{2,i},\mu_i)$组成的列表$L_3$。当$\mathcal{A}$对$(id_i,T_i,C_i',S_i,T_{1,i},T_{2,i})$进行$H_3$询问时，如果$(id_i,T_i,C_i',S_i,T_{1,i},T_{2,i},\mu_i)$存在于$L_3$，$\mathcal{B}$返回$\mu_i$给$\mathcal{A}$；否则，$\mathcal{B}$随机选择$\zeta_i\in\mathbb{Z}_N^*$，插入$(id_i,T_i,C_i',S_i,T_{1,i},T_{2,i},\mu_i)$到$L_3$中，并返回$\mu_i$给$\mathcal{A}$。

(5) 私钥提取询问：当$\mathcal{A}$对满足$id_i\neq id^*$的id_i进行私钥提取询问时，$\mathcal{B}$计算$SK_{id_i}=h_0^{a\prod_{j=1,j\neq i}^{k}(a+\kappa_j)}$并返回给$\mathcal{A}$。

(6) 重加密密钥提取询问：当$\mathcal{A}$对满足$id_i\neq id^*$的(id_i,S_i)进行重加密密钥提取询问时，$\mathcal{B}$运行 Re-KeyGen(SK_{id_i},S_i)生成重加密密钥$rk_{id_i\to S_i}$并返回给$\mathcal{A}$。

挑战：$\mathcal{A}$输出两个消息(m_0^*,m_1^*)作为挑战，$\mathcal{B}$执行：

① 随机选择$b\in\{0,1\}$，$\chi^*\in\mathbb{G}_T$。

② 计算

$$c_0^*=\chi^*\cdot Z^{\prod_{i=k+2}^{k+n}\kappa_i}\cdot e\left(g_0^{\left(\prod_{i=k+2}^{k+n}(a+\kappa_i)-\prod_{i=k+2}^{k+n}\kappa_i\right)/a},h_0^{\nu a^2Q(a)}\right),$$

$$c_1^*=g_0^{\nu P(a)},$$

$$c_2^*=h_0^{w\cdot\nu a^2Q(a)},$$

$$c_3^*=m_b^*\oplus KDF(\chi^*)。$$

③ 返回挑战密文$C_b^*=\{c_0^*,c_1^*,c_2^*,c_3^*\}$给$\mathcal{A}$。

询问 2：$\mathcal{A}$继续进行询问 1 中的询问。

猜测：$\mathcal{A}$输出猜测b'。若$b'=b$，$\mathcal{A}$赢得游戏。

如果$Z=e(g_0,h_0)^{\nu aQ(a)}$，那么

$$\begin{aligned}c_0^*&=\chi^*\cdot Z^{\prod_{i=k+2}^{k+n}\kappa_i}\cdot e\left(g_0^{\left(\prod_{i=k+2}^{k+n}(a+\kappa_i)-\prod_{i=k+2}^{k+n}\kappa_i\right)/a},h_0^{\nu a^2Q(a)}\right)\\&=\chi^*\cdot e(g_0,h_0)^{\nu aQ(a)\prod_{i=k+2}^{k+n}\kappa_i}\cdot e\left(g_0^{\left(\prod_{i=k+2}^{k+n}(a+\kappa_i)-\prod_{i=k+2}^{k+n}\kappa_i\right)},h_0^{\nu aQ(a)}\right)\\&=\chi^*\cdot e(g_0^{\prod_{i=k+2}^{k+n}(a+\kappa_i)},h_0^{\nu aQ(a)})=\chi^*\cdot\sigma^{\nu},\end{aligned}$$

$$\begin{aligned}c_1^*&=g_0^{\nu P(a)}=g^{\nu\prod_{i=k+1}^{k+n}(a+\kappa_i)}=g_0^{\nu(a+\kappa_{k+1})\cdot\prod_{i=k+2}^{k+n}(a+\kappa_i)}\\&=g^{\nu(a+\kappa_{k+1})}=g^{\nu(a+H(id^*\|hid,N))},\end{aligned}$$

$$c_2^*=h_0^{\omega\cdot\nu a^2Q(a)}=u^{\nu}。$$

因此，C_b^*是有效密文，则$\Pr[b'=b]=\frac{1}{2}+\xi$。

如果$Z\neq e(g_0,h_0)^{\nu aQ(a)}$，由于$Z$是$\mathbb{G}_T$中随机元素，那么$C_b^*$也是随机的，则$\Pr[b'=b]=\frac{1}{2}$。

因此，$\mathcal{B}$解(P,Q)-GDDHE 问题的优势为

$$\begin{aligned}\xi'&=|\Pr[b'=b|Z=e(g_0,h_0)^{\nu aQ(a)}]-\\&\quad\Pr[b'=b|Z\neq e(g_0,h_0)^{\nu aQ(a)}]|\\&=\left|\frac{1}{2}+\xi-\frac{1}{2}\right|=\xi。\end{aligned}$$

证毕。

引理 2. 假定攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ξ 赢得游戏 IND-sID-CPA-II，则存在算法 $\mathcal{B}$ 能够以不可忽略的优势 ξ' 解 (P,Q)-GDDHE 问题。

证明. 给定 (P,Q)-GDDHE 实例 $\{g_0, g_0^a, g_0^{a^2}, \cdots, g_0^{a^{2n}}, g_0^{\nu P(a)}, h_0^a, h_0^{a^2}, \cdots, h_0^{a^k}, h_0^{a^2 Q(a)}, h_0^{\nu a^2 Q(a)}, Z\}$，$\mathcal{B}$ 的目标是判断 $Z=e(g_0,h_0)^{\nu a Q(a)}$ 是否成立，其中 $P(x)=\prod_{i=k+1}^{k+n}(x+\kappa_i)$ 和 $Q(x)=\prod_{i=1}^{k}(x+\kappa_i)$ 是两个互质多项式，$\kappa_1,\cdots,\kappa_{n+k}\in\mathbb{Z}_N^*$。

初始化：$\mathcal{A}$ 输出挑战标识集合 $S^*=\{id_1^*,\cdots,id_\eta^*\}(\eta\leq n)$。

系统建立：$\mathcal{B}$ 隐式设置 $\alpha=a$，$h=h_0^{Q(a)}$，随机选择 $u\in\mathbb{G}_2$，计算 $g=g_0^{\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)}$，$h_2=h_0^{a^2Q(a)}$，$g^a=g_0^{a\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)}$，$g^{a^2}=g_0^{a^2\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)}$，$\cdots$，$g^{a^n}=g_0^{a^n\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)}$，$\sigma=e(g_0^{\prod_{i=1}^{k}(a+\kappa_i)\cdot\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)},h_0^a)$。$\mathcal{B}$ 选择密钥生成函数标识 hid，密钥派生函数 $KDF:\{0,1\}^*\to\{0,1\}^l$，返回系统参数 $params$ 给 $\mathcal{A}$。

询问 1：$\mathcal{A}$ 能够适应性地进行以下询问：

(1) H 询问：$\mathcal{B}$ 维护初始为空的由元组 (id_i,κ_i) 组成的列表 L。当 $\mathcal{A}$ 对 id_i 进行 H 询问时，如果 (id_i,κ_i) 存在于 L，$\mathcal{B}$ 返回 κ_i 给 $\mathcal{A}$；否则，$\mathcal{B}$ 执行：

① 如果 $id_i\in S^*$，$\mathcal{B}$ 随机选择 $\kappa_i\in[\kappa_{k+1},\kappa_{k+s}]$，插入 (id_i,κ_{k+1}) 到 L 中，并返回 κ_i 给 $\mathcal{A}$。

② 如果 $id_i\notin S^*$，$\mathcal{B}$ 随机选择 $\kappa_i\in[\kappa_1,\kappa_k]$，插入 (id_i,κ_i) 到 L 中，并返回 κ_i 给 $\mathcal{A}$。

(2) H_1 询问：与引理 1 相同。

(3) H_2 询问：与引理 1 相同。

(4) H_3 询问：与引理 1 相同。

(5) 私钥提取询问：当 $\mathcal{A}$ 对满足 $id_i\notin S^*$ 的标识 id_i 进行私钥提取询问时，$\mathcal{B}$ 计算 $SK_{id_i}=h_0^{a\prod_{j=1,j\neq i}^{k}(a+\kappa_j)}$ 并返回给 $\mathcal{A}$。

(6) 重加密密钥提取询问：当 $\mathcal{A}$ 对满足 $id_i\notin S^*$ 的 (id_i,S_i) 进行重加密密钥提取询问时，$\mathcal{B}$ 运行 Re-KeyGen(SK_{id_i},S_i) 生成 $rk_{id_i\to S_i}$ 并返回给 $\mathcal{A}$。

挑战：$\mathcal{A}$ 输出两个消息 (m_0^*,m_1^*) 和用户标识 id 作为挑战，$\mathcal{B}$ 执行：

① 随机选择 $b\in\{0,1\}$，$\chi^*\in\mathbb{G}_T$，$t_2^*\in\mathbb{Z}_N^*$。

② 计算

$$T^*=Z^{\prod_{i=k+\eta+1}^{k+n}\kappa_i}\cdot e\left(g_0^{\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)-\prod_{i=k+\eta+1}^{k+n}\kappa_i}\right)^{1/a},h_0^{\nu a^2Q(a)}),$$

$$r^*=H_1(m_b^*\|\chi^*,N),$$

$$k^*=H_2(T^*),$$

$$c_0'^*=\chi^*\cdot e(g^{r^*\cdot(a+H(id\|hid,N))},u^{t_2^*\cdot k^*})^{-1},$$

$$c_1'^*=g^{t_2^*\cdot(a+H(id\|hid,N))},$$

$$c_2'^*=u^{r^*},$$

$$c_3'^*=g_0^{\nu P(a)},$$

$$c_4'^*=m_b^*\oplus KDF(\chi^*),$$

$$c_5'^*=h_0^{\nu a^2Q(a)}。$$

③ 返回挑战密文 $C_b'^*=\{c_0'^*,c_1'^*,c_2'^*,c_3'^*,c_4'^*,c_5'^*\}$ 给 $\mathcal{A}$。

询问 2：$\mathcal{A}$ 继续进行询问 1 中的询问。

猜测：$\mathcal{A}$ 输出猜测 b'。若 $b'=b$，$\mathcal{A}$ 赢得游戏。

如果 $Z=e(g_0,h_0)^{\nu aQ(a)}$，那么

$$\begin{aligned}T^*&=Z^{\prod_{i=k+\eta+1}^{k+n}\kappa_i}\cdot e\left(g_0^{\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)-\prod_{i=k+\eta+1}^{k+n}\kappa_i}\right)^{1/a},h_0^{\nu a^2Q(a)})\\&=e(g_0,h_0)^{\nu aQ(a)\prod_{i=k+\eta+1}^{k+n}\kappa_i}\cdot e\left(g_0^{\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)-\prod_{i=k+\eta+1}^{k+n}\kappa_i},h_0^{\nu aQ(a)}\right)\\&=e(g_0^{\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)},h_0^{\nu aQ(a)})=\sigma^\nu,\end{aligned}$$

$$\begin{aligned}c_3'^*&=g_0^{\nu P(a)}=g_0^{\nu\prod_{i=k+1}^{k+n}(a+\kappa_i)}=g_0^{\nu\prod_{i=k+1}^{k+\eta}(a+\kappa_i)\cdot\prod_{i=k+\eta+1}^{k+n}(a+\kappa_i)}\\&=g^{\nu\prod_{i=k+1}^{k+\eta}(a+\kappa_i)}=g^{\nu\cdot\prod_{l=1}^{\eta}(a+H(id_l^*\|hid,N))},\end{aligned}$$

$$c_5'^*=h_0^{\nu a^2Q(a)}=h_2^\nu。$$

因此，$C_b'^*$ 是有效密文，则 $\Pr[b'=b]=\frac{1}{2}+\xi$。

如果 $Z\neq e(g_0,h_0)^{\nu aQ(a)}$，由于 Z 是 $\mathbb{G}_T$ 中随机元素，那么 $C_b'^*$ 也是随机的，则 $\Pr[b'=b]=\frac{1}{2}$。

因此，$\mathcal{B}$ 解 (P,Q)-GDDHE 问题的优势为

$$\begin{aligned}\xi'&=|\Pr[b'=b|Z=e(g_0,h_0)^{\nu aQ(a)}]-\\&\quad\Pr[b'=b|Z\neq e(g_0,h_0)^{\nu aQ(a)}]|\\&=\left|\frac{1}{2}+\xi-\frac{1}{2}\right|=\xi。\end{aligned}$$

证毕。

定理 3. 如果 q-SDH 假设成立，则所提方案在随机预言机模型中是 SKLR-CA 安全的。

证明. 假定攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ξ 赢得游戏 SKLR-CA，则存在算法 $\mathcal{B}$ 能够以不可忽略的优势 ξ' 解 q-SDH 问题。给定 q-SDH 实例 $\{g_0,$

$h_0, h_0^a, h_0^{a^2}, \cdots, h_0^{a^q}\}$，$\mathcal{B}$ 的目标是寻找 $\{\nu, g_0^{1/(a+\nu)}\}$，其中 $\nu \in \mathbb{Z}_N^*$。

初始化：$\mathcal{A}$ 输出挑战标识 id^*。

系统建立：$\mathcal{B}$ 隐式设置 $\alpha = a, n < q$，随机选择 $\kappa_1, \cdots, \kappa_{q-1}, \omega, \theta \in \mathbb{Z}_N^*$，计算 $u = h_0$，$g = \varphi(h_0^\theta)$，$h = h_0^{\prod_{i=1}^{q-2}(a+\kappa_i)}$，$h_2 = h_0^{a^2\prod_{i=1}^{q-2}(a+\kappa_i)}$，$g = \varphi(h_0^\theta)$，$g^a = \varphi(h_0^{\theta a})$，$g^{a^2} = \varphi(h_0^{\theta a^2})$，$\cdots$，$g^{a^n} = \varphi(h_0^{\theta a^n})$，$\sigma = e(g, h_0^{a\prod_{i=1}^{q-2}(a+\kappa_i)})$，$\mathcal{B}$ 选择密钥生成函数标识 hid，密钥派生函数 $KDF: \{0,1\}^* \to \{0,1\}^l$，返回系统参数 $params$ 给 $\mathcal{A}$。

询问 1：$\mathcal{A}$ 能够适应性地进行以下询问：

(1) H 询问：$\mathcal{B}$ 维护初始为空的由元组 (id_i, κ_i) 组成的列表 L。当 $\mathcal{A}$ 对 id_i 进行 H 询问时，如果 (id_i, κ_i) 存在于 L，$\mathcal{B}$ 返回 κ_i 给 $\mathcal{A}$；否则，$\mathcal{B}$ 执行：

① 如果 $id_i = id^*$，$\mathcal{B}$ 插入 (id_i, κ_{q-1}) 到 L 中，并返回 κ_{k+1} 给 $\mathcal{A}$。

② 如果 $id_i \neq id^*$，$\mathcal{B}$ 随机选择 $\kappa_i \in [\kappa_1, \kappa_{q-2}]$，插入 (id_i, κ_i) 到 L 中，并返回 κ_i 给 $\mathcal{A}$。

(2) H_1 询问：与引理 1 相同。

(3) H_2 询问：与引理 1 相同。

(4) H_3 询问：与引理 1 相同。

(5) 私钥提取询问：当 $\mathcal{A}$ 对满足 $id_i \neq id^*$ 的 id_i 进行私钥提取询问时，$\mathcal{B}$ 计算 $SK_{id_i} = h_0^{a\prod_{j=1,j\neq i}^{q-2}(a+\kappa_j)}$ 并返回给 $\mathcal{A}$。

(6) 重加密密钥提取询问：当 $\mathcal{A}$ 对 (id_i, S_i) 进行重加密密钥提取询问时满足 $S_i = \{id_1, \cdots, id_{\eta_i}\}$ $(\eta_i \leq n)$，$\mathcal{B}$ 执行：

① 如果 $id_i = id^*$，$\mathcal{B}$ 随机选择 $t_1, t_2' \in \mathbb{Z}_N^*$，隐式设置 $t_2 = \left(t_2' - a\prod_{i=1}^{q-2}(a+\kappa_i)/(a+\kappa_{q-1})\right)\Big/k$，计算 $T = \sigma^{t_1}$，$k = H_2(T)$，$rk_0 = u^{t_2'}$，$rk_1 = g^{\left(t_2'\cdot(a+\kappa_{q-1}) - a\prod_{i=1}^{q-2}(a+\kappa_i)\right)/k}$，$rk_2 = \varphi(h_0^{\theta_1\cdot\prod_{l=1}^{\eta_i}(a+H(id_l\|hid,N))})$，$rk_3 = h_2^{t_1}$，返回 $rk_{id_i\to S_i} = \{rk_0, rk_1, rk_2, rk_3\}$ 给 $\mathcal{A}$。

② 如果 $id_i \neq id^*$，$\mathcal{B}$ 运行 Re-KeyGen(SK_{id_i}, S_i) 生成 $rk_{id_i\to S_i}$ 并返回给 $\mathcal{A}$。

输出：$\mathcal{A}$ 输出满足 $e(g^{a+\kappa_{q-1}}, SK^*) = \sigma$ 的私钥 SK^*。定义多项式 $F(x) = x\prod_{i=1}^{q-2}(x+\kappa_i)$，可表示为 $F(x) = (x+\kappa_{q-1})\cdot f(x) + \gamma$，其中 $f(x) = \sum_{i=0}^{q-2} f_i x^i$，$f_0, \cdots, f_{q-2}, \gamma \in \mathbb{Z}_N^*$。$\mathcal{B}$ 输出 $\{\kappa_{q-1}, \varphi((SK^*/h_0^{-f(a)})^{1/\gamma})\}$ 为 q-SDH 实例的解。

由于 $SK^* = h^{a/(a+\kappa_{q-1})} = h_0^{F(a)/(a+\kappa_{q-1})}$，那么

$$\varphi((SK^*/h_0^{-f(a)})^{1/\gamma}) = \varphi(h_0^{(F(a)/(a+\kappa_{q-1})-f(a))/\gamma}) = \varphi(h^{(\gamma/(a+\kappa_{q-1}))/\gamma_0}) = g_0^{1/(a+\kappa_{q-1})}。$$

因此，$\mathcal{B}$ 解 q-SDH 问题的优势为 $\xi' = \xi$。

证毕。

定理 4.　如果哈希函数抗碰撞假设成立，则所提方案满足可验证性。

证明.　假定攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ξ 赢得游戏 Verifiability，则存在算法 $\mathcal{B}$ 能够以不可忽略的优势 ξ' 打破 H_1 的抗碰撞性。给定密码哈希函数实例 $\mathcal{H}$，$\mathcal{B}$ 的目标是寻找 $\mathcal{H}$ 的一对碰撞。

系统建立：$\mathcal{B}$ 运行 Setup 算法生成系统参数 $params$ 和主私钥 msk，设置 H_1 为 $\mathcal{H}$，将 $params$ 发送给 $\mathcal{A}$。

询问 1：$\mathcal{A}$ 能够适应性地进行以下询问：

① 私钥提取询问：当 $\mathcal{A}$ 对 id_i 进行私钥提取询问时，$\mathcal{B}$ 运行 Extract 算法生成 SK_{id_i} 并返回给 $\mathcal{A}$。

② 重加密密钥提取询问：当 $\mathcal{A}$ 对 (id_i, S_i) 进行重加密密钥提取询问时，$\mathcal{B}$ 运行 Re-KeyGen 算法生成重加密密钥 $rk_{id_i\to S_i}$ 并返回给 $\mathcal{A}$。

挑战：$\mathcal{A}$ 输出消息 m^*，用户标识 id^* 和授权用户标识集合 S^* 作为挑战，$\mathcal{B}$ 随机选取 $\chi^* \in \mathbb{G}_T$，计算 $r^* = \mathcal{H}(m^*\|\chi^*, N)$，$c_0^* = \sigma^{r^*}\cdot\chi^*$，$c_1^* = g^{r^*\cdot(\alpha+H(id^*\|hid,N))}$，$c_2^* = u^{r^*}$，$c_3^* = m^* \oplus KDF(\chi^*)$，运行 Re-KeyGen 算法生成 $rk_{id^*\to S^*}$。$\mathcal{B}$ 返回挑战密文 $C^* = \{c_0^*, c_1^*, c_2^*, c_3^*\}$ 和 $rk_{id^*\to S^*}$ 给 $\mathcal{A}$。

输出：$\mathcal{A}$ 输出重加密密文 $C'^* = \{c_0'^*, c_1'^*, c_2'^*, c_3'^*, c_4'^*\}$。$\mathcal{B}$ 随机选择 $id \in S^*$，运行 Extract 算法生成 SK_{id}，运行 DecVerify 算法生成 m'^* 和 χ'^*，输出 $\{m^*\|\chi^*, m'^*\|\chi'^*\}$ 为 $\mathcal{H}$ 的一对碰撞。

由于 DecVerify$(SK_{id}, C'^*, S^*) = m'^*$，那么 $u^{\mathcal{H}(m'^*\|\chi'^*,N)} = u^{\mathcal{H}(m^*\|\chi^*,N)}$。

因此，$\mathcal{B}$ 打破 H_1 的抗碰撞性的优势为 $\xi' = \xi$。

证毕。

定理 5.　如果零知识证明系统 Π 满足可靠性，则所提方案满足公平性。

证明.　假定攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ξ 赢得游戏 Fairness，则算法 $\mathcal{B}$ 能够以不可忽略的优势 ξ' 打破 Π 的可靠性。

系统建立：$\mathcal{B}$ 运行 Setup 算法生成系统参数

$params$ 和主私钥 msk，将 $params$ 发送给 $\mathcal{A}$。

询问 1：与定理 3 相同。

挑战：$\mathcal{A}$ 输出消息 m^*，用户标识 id 和授权用户标识集合 $S^*=\{id_1^*,\cdots,id_\eta^*\}(\eta\leq n)$ 作为挑战，$\mathcal{B}$ 执行：

① 随机选择 $\chi^*\in\mathbb{G}_T$，$t_1^*,t_2^*\in\mathbb{Z}_N^*$。

② 计算

$$r^*=H_1(m_b^*\|\chi^*,N),$$

$$T^*=\sigma^{t_1^*},$$

$$k^*=H_2(T^*),$$

$$c_0'^*=\chi^*\cdot e(g^{r^*\cdot(\alpha+H(id\|hid,N))},u^{t_2^*\cdot k^*})^{-1},$$

$$c_1'^*=g^{t_2^*\cdot(\alpha+H(id\|hid,N))},$$

$$c_2'^*=u^{r^*},$$

$$c_3'^*=g^{t_1^*\cdot\prod_{l=1}^{\eta}(\alpha+H(id_l^*\|hid,N))},$$

$$c_4'^*=m^*\oplus KDF(\chi^*),$$

$$c_5'^*=h_2^{t_1^*}。$$

③ 返回挑战密文 $C'^*=\{c_0'^*,c_1'^*,c_2'^*,c_3'^*,c_4'^*,c_5'^*\}$ 给 $\mathcal{A}$。

输出：$\mathcal{A}$ 输出错误报告 $\pi^*=\{T'^*,c^*,res^*\}$ 和授权用户标识 id^*，$\mathcal{B}$ 转发该输出。

由于 $\mathrm{Claim}(id^*,C'^*,\pi^*,S^*)=1$ 且 $T'^*\neq T^*$，则 π^* 是一个错误陈述的有效证明。

因此，$\mathcal{B}$ 打破 Π 的可靠性的优势为 $\xi'=\xi$。

证毕。

6 性能分析

本节对所提方案与文献[20-21]中方案进行性能分析，包括计算代价和存储代价。

6.1 理论分析

表 2 给出理论分析结果，其中 t_p，t_e，t_{sm1}，t_{sm2}，t_H 分别表示双线性映射运算，$\mathbb{G}_T$ 上指数运算，$\mathbb{G}_1$ 上标量乘运算，$\mathbb{G}_2$ 上标量乘运算和 Map-to-Point 哈希运算所需时间；η 为授权用户数量；$|\mathbb{G}_T|$、$|\mathbb{G}_1|$、$|\mathbb{G}_2|$、$|\mathbb{Z}_q^*|$ 和 $|m|$ 分别表示 $\mathbb{G}_T$、$\mathbb{G}_1$、$\mathbb{G}_2$、$\mathbb{Z}_q^*$ 中元素和消息长度；$|SK|$、$|rk|$、$|C|$、$|C'|$ 分别表示用户私钥、重加密密钥、初始密文和重加密密文长度。

表 2 理论分析

		文献[20]	文献[21]	所提方案
计算代价	Encrypt	t_e+6t_{sm1}	$t_e+4t_{sm1}+3t_{sm2}+t_H$	$t_e+2t_{sm1}+t_{sm2}$
	Re-KeyGen	$2t_e+(2\eta+3)t_{sm1}+7t_{sm2}+t_H$	$2t_e+(\eta+3)t_{sm1}+2t_{sm2}+t_H$	$t_e+(\eta+2)t_{sm1}+2t_{sm2}$
	Re-Encrypt	$3t_p+t_{sm1}$	t_p	t_p
	Decrypt	$3t_p+3t_{sm1}$	t_p+2t_{sm1}	t_p
	DecVerify	$4t_p+t_e+(s+2)t_{sm1}+t_H$	$5t_p+t_e+2t_{sm1}+(\eta-1)t_{sm2}+2t_H$	$3t_p+\eta t_{sm1}+2t_{sm2}$
	Claim	$3t_p+2t_e+2t_{sm1}+t_H$	$4t_p+t_e+3t_{sm1}$	$4t_p+2t_e+(\eta+2)t_{sm1}+2t_{sm2}$
存储代价	$\|SK\|$	$3\|\mathbb{G}_2\|$	$\|\mathbb{G}_1\|$	$\|\mathbb{G}_2\|$
	$\|C\|$	$4\|\mathbb{G}_1\|+2\|m\|$	$\|\mathbb{G}_T\|+3\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|m\|$	$\|\mathbb{G}_T\|+\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|m\|$
	$\|rk\|$	$2\|\mathbb{G}_T\|+(\eta+3)\|\mathbb{G}_1\|+4\|\mathbb{G}_2\|+\|\mathbb{Z}_N^*\|$	$\|\mathbb{G}_T\|+3\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|$	$2\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|$
	$\|C'\|$	$3\|\mathbb{G}_T\|+(\eta+5)\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{Z}_N^*\|+2\|m\|$	$2\|\mathbb{G}_T\|+6\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|+\|m\|$	$\|\mathbb{G}_T\|+2\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|+\|m\|$

从表 2 可以看出，所提方案中 Encrypt、Re-KeyGen、Decrypt 和 DecVerify 算法的计算代价均优于文献[20-21]；Re-Encrypt 算法的计算代价与文献[21]相当，优于文献[20]。所提方案中 Claim 算法的计算代价与授权用户数量 η 相关，而文献[20-21]保持恒定。综上所述，相比于文献[20-21]，除 Claim 算法以外，所提方案的计算代价均达到最低。所提方案中用户私钥长度低于文献[20]。在初始密文长度方面，当 $|m|$ 较小时，文献[20]优于所提方案和文献[21]；当 $|m|$ 较大时，所提方案优于文献[20-21]。在重加密密钥和重加密密文长度方面，所提方案取得了最优的存储代价，文献[21]与所提方案实现恒定长度，而文献[20]与授权用户数量 η 相关。故所提方案在存储代价方面也存在优势。

6.2 仿真实验

为评估实际运行环境中方案性能，在 128-bits 安全性下，基于 Java 语言和 JPBC 密码学库，使用 SM9 推荐曲线[22]对所提方案与文献[20-21]中方案进行仿真实现。测试环境为 Windows 操作系统，配有 12 核 i5-10400@2.90 GHz 处理器和 16 GB RAM。$\mathbb{G}_T$，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{Z}_q^*$ 中元素长度分别为 3072、512、1024、256 bits。设定消息长度为 256 bits。图 2 给出了所提方案与文献[20-21]中方案的仿真实验结果。

如图 2(a)所示，所提方案中 Encrypt、Re-Encrypt

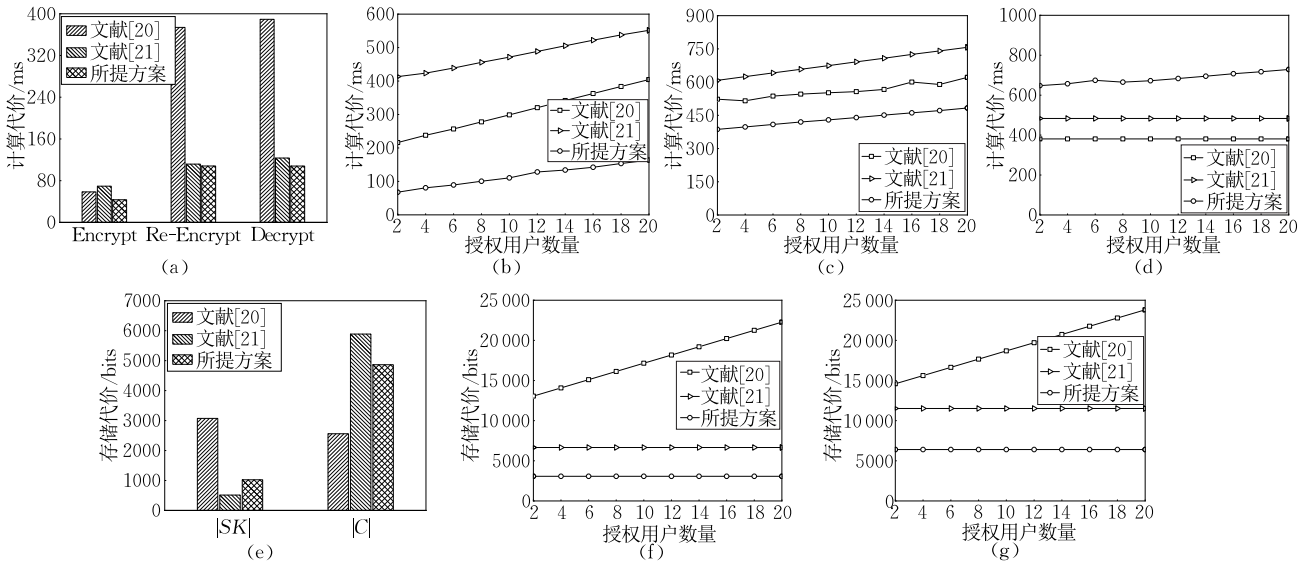

图 2　仿真实验比较((a) Encrypt、Re-Encrypt 和 Decrypt 算法的计算代价；(b) Re-KeyGen 算法的计算代价；(c) DecVerify 算法的计算代价；(d) Claim 算法的计算代价；(e) 用户私钥和初始密文的存储代价；(f) 重加密密钥的存储代价；(g) 重加密密文的存储代价)

和 Decrypt 算法均比文献[20-21]更加高效。具体来说，所提方案 Encrypt 算法需要 43.41 ms，Re-Encrypt 算法需要 108.17 ms，Decrypt 算法需要 108.06 ms；而文献[20]需要 58.51、373.86 和 389.41 ms；文献[21]需要 69.44、111.81 和 123.38 ms。因此，相比于文献[20-21]，所提方案分别降低了 25.81% 和 37.49% 的 Encrypt 算法计算代价，降低了 71.07% 和 3.26% 的 Re-Encrypt 算法计算代价，降低了 72.25% 和 12.42% 的 Decrypt 算法计算代价。从图 2(b)和图 2(c)可以看出，文献[20-21]和所提方案中 Re-KeyGen 和 DecVerify 算法的计算代价与授权用户数量 η 之间均呈现正相关关系。然而，所提方案中效率优于文献[20-21]。具体来说，当 $s=20$ 时，所提方案中 Re-KeyGen 算法需要 163.72 ms，而文献[20-21]分别需要 404.35 和 551.67 ms。与文献[20-21]相比，所提方案能够节约 59.51% 和 70.32% 的计算代价。所提方案中 DecVerify 算法需要 483.06 ms，而文献[20-21]分别需要 621.46 和 757.22 ms。与文献[20-21]相比，所提方案能够节约 22.27% 和 36.21% 的计算代价。图 2(d)所示，所提方案中 Claim 算法计算代价略高于文献[20-21]。主要原因是所提方案采用零知识证明技术实现公平性，该过程需要验证解密操作的正确性，造成计算代价增加。然而，在文献[20-21]中，Claim 算法需要输入初始密文、重加密密钥、重加密密文和错误报告以验证云服务器的行为，因此需要保证验证者可信，同时该算法产生高额通信成本。相比之下，所提方案中 Claim 算法仅需输入重加密密文和错误报告，且不泄露任何隐私信息给验证者，因此可实现公开可验证。总体而言，所提方案实现了更完备的可验证性，同时极大减轻用户与云服务器的计算代价。

由图 2(e)可知，所提方案中用户私钥存储代价低于文献[20]，初始密文存储代价低于文献[21]。具体地，所提方案中用户私钥为 1024 bits，而文献[20]为 3072 bits，故所提方案降低 66.67% 的用户私钥存储代价；所提方案中初始密文为 4864 bits，而文献[21]为 5888 bits，故所提方案降低 17.39% 的初始密文存储代价。图 2(f)和图 2(g)表明，所提方案和文献[21]中重加密密钥和重加密密文的存储代价恒定，而文献[20]随授权用户数量 η 增加。具体来说，当 $\eta=20$ 时，所提方案中重加密密钥和重加密密文分别为 3072 和 6400 bits，而文献[20]为 22272 和 23 808 bits，文献[21]为 6656 和 11 520 bits。所提方案比文献[20-21]分别降低了 86.21% 和 53.85% 的重加密密钥存储代价，降低了 73.12% 和 44.44% 的重加密密文存储代价。因此，所提方案在多用户数据共享过程中显著降低了云服务器的存储代价，具备更好的实用性。

7　总　结

针对 SM9 算法不支持密文转换和仅适用于单用

户场景、代理重加密中不可信代理者返回错误密文问题，本文提出基于 SM9 的可验证公平标识广播代理重加密方案，使得数据拥有者以可验证的方式一次性与多个授权用户共享密文数据。基于 Fujisaki-Okamoto 转换和零知识证明技术，所提方案实现了可验证性和公平性。本文优化可验证公平标识广播代理重加密的形式化定义和安全模型，并在随机预言机模型下证明所提方案的安全性。通过全面的理论和实验分析比较，验证了所提方案相比于已有方案在计算代价和存储代价方面的有效性和实用性。

尽管所提方案能够实现更完备的安全性并在效率方面相比于已有方案存在优势，但是所提方案不支持细粒度访问控制，缺乏考虑密文中身份隐私泄漏问题。未来工作可围绕增强身份隐私性和提高访问控制级别两方面展开。

参 考 文 献

[1] Abu-Libdeh H, Princehouse L, Weatherspoon H. RACS: A case for cloud storage diversity//Proceedings of the ACM Symposium on Cloud Computing. New York, USA, 2010: 229-240

[2] Kamara S, Lauter K. Cryptographic cloud storage//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2010, 6054: 136-149

[3] Wei L, Zhu H, Cao Z, et al. Security and privacy for storage and computation in cloud computing. Information Sciences, 2014, 258: 371-386

[4] Feng Deng-Guo, Zhang Min, Zhang Yan, et al. Study on cloud computing security. Journal of Software, 2011, 22(1): 71-83(in Chinese)
(冯登国，张敏，张妍等. 云计算安全研究. 软件学报，2011，22(1)：71-83)

[5] Feng Chao-Sheng, Qin Zhi-Guang, Yuan Ding. Techniques of secure storage for cloud data. Chinese Journal of Computers, 2015, 38(1): 150-163(in Chinese)
(冯朝胜，秦志光，袁丁. 云数据安全存储技术. 计算机学报，2015，38(1)：150-163)

[6] Shen Jian, Zhou Tian-Qi, Cao Zhen-Fu. Protection methods for cloud data security. Journal of Computer Research and Development, 2021, 58(10): 2079-2098(in Chinese)
(沈剑，周天祺，曹珍富. 云数据安全保护方法综述. 计算机研究与发展，2021，58(10)：2079-2098)

[7] Liu H, Ming Y, Wang C, et al. Blockchain-assisted verifiable certificate-based searchable encryption against untrusted cloud server for Industrial Internet of Things. Future Generation Computer Systems, 2024, 153: 97-112

[8] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography//Proceedings of the Advances in Cryptology-EUROCRYPT'98. Berlin, Germany: Springer, 1998, 1403: 127-144

[9] Green M, Ateniese G. Identity-based proxy re-encryption//Proceedings of the International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer, 2007: 288-306

[10] Boneh D, Franklin M. Identity-based encryption from the weil pairing//Proceedings of the Advances in Cryptology-CRYPTO'01. Berlin, Germany: Springer, 2001, 2139: 213-229

[11] Xu P, Jiao T, Wu Q, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Transactions on Computers, 2015, 65(1): 66-79

[12] Deng H, Qin Z, Wu Q, et al. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Transactions on Information Forensics and Security, 2020, 15: 3168-3180

[13] Ge C, Liu Z, Xia J, et al. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. IEEE Transactions on Dependable and Secure Computing, 2019, 18(3): 1214-1226

[14] Deng H, Zhang J, Qin Z, et al. Policy-based broadcast access authorization for flexible data sharing in clouds. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 3024-3037

[15] Maiti S, Misra S. P2B: Privacy preserving identity-based broadcast proxy re-encryption. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5610-5617

[16] Zhang J, Su S, Zhong H, et al. Identity-based broadcast proxy re-encryption for flexible data sharing in VANETs. IEEE Transactions on Information Forensics and Security, 2023, 18: 4830-4842

[17] Sun J, Xu G, Zhang T, et al. Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(7): 7527-7540

[18] Ohata S, Kawai Y, Matsuda T, et al. Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption//Proceedings of the Cryptographers' Track at the RSA Conference. Cham, Cambodia: Springer, 2015, 9048: 410-428

[19] Ge C, Susilo W, Baek J, et al. A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 2907-2919

[20] Sun J, Xu G, Zhang T, et al. Verifiable, fair and privacy-preserving broadcast authorization for flexible data sharing in clouds. IEEE Transactions on Information Forensics and Security, 2023, 18: 683-698

[21] Jiang L, Alazab M, Qin Z. Secure task distribution with verifiable re-encryption in mobile crowdsensing assisted emergency IoT system. IEEE Internet of Things Journal, 2023, 11(3): 3896-3908

[22] GM/T0044-2016. SM9 identity-based cryptographic algorithms. State Cryptography Administration, 2016(in Chinese)
(GM/T0044-2016. SM9 标识密码算法. 国家密码管理局, 2016)

[23] Lai Jian-Chang, Huang Xin-Yi, He De-Biao. An efficient identity-based broadcast encryption scheme based on SM9. Chinese Journal of Computers, 2021, 44(5): 897-907(in Chinese)
(赖建昌, 黄欣沂, 何德彪. 一种基于商密 SM9 的高效标识广播加密方案. 计算机学报, 2021, 44(5): 897-907)

[24] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. CCA secure broadcast encryption based on SM9. Journal of Software, 2023, 34(7): 3354-3364(in Chinese)
(赖建昌, 黄欣沂, 何德彪等. 基于 SM9 的 CCA 安全广播加密方案. 软件学报, 2023, 34(7): 3354-3364)

[25] Cui Yan, Huang Xin-Yi, Lai Jian-Chang, et al. Anonymous broadcast encryption based on SM9. Journal of Cyber Security, 2023, 8(6): 15-27(in Chinese)
(崔岩, 黄欣沂, 赖建昌等. 基于 SM9 的匿名广播加密方案. 信息安全学报, 2023, 8(6): 15-27)

[26] Liu H, Ming Y, Wang C, et al. Identity-based proxy re-encryption based on SM9//Proceedings of the International Conference on Information Security and Cryptology. Singapore: Springer, 2023, 14526: 320-339

[27] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Proceedings of the Advances in Cryptology-CRYPTO'99. Berlin, Germany: Springer, 1999, 1666: 537-554

[28] Weng J, Deng R H, Ding X, et al. Conditional proxy re-encryption secure against chosen-ciphertext attack//Proceedings of the International Symposium on Information, Computer, and Communications Security. New York, USA, 2009: 322-332

[29] Guo H, Zhang Z, Xu J, et al. Accountable proxy re-encryption for secure data sharing. IEEE Transactions on Dependable and Secure Computing, 2018, 18(1): 145-159

[30] Zhou Y, Liu S, Han S, et al. Fine-Grained proxy re-encryption: Definitions and constructions from LWE//Proceedings of the Advances in Cryptology-ASIACRYPT'99. Singapore: Springer, 2023, 14443: 199-231

[31] Tang Q, Hartel P, Jonker W. Inter-domain identity-based proxy re-encryption//Proceedings of the International Conference on Information Security and Cryptology. Berlin, Germany: Springer, 2008, 5487: 332-347

[32] Wang H, Cao Z, Wang L. Multi-use and unidirectional identity-based proxy re-encryption schemes. Information Sciences, 2010, 180(20): 4042-4059

[33] Wang L, Wang L, Mambo M, et al. New identity-based proxy re-encryption schemes to prevent collusion attacks//Proceedings of the International Conference on Pairing-Based Cryptography. Berlin, Germany: Springer, 2010, 6487: 327-346

[34] Liang K, Liu J K, Wong D S, et al. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing//Proceedings of the European Symposium on Research in Computer Security. Cham, Cambodia: Springer, 2014, 8712: 257-272

[35] Lin X, Lu R. Proxy re-encryption with delegatable verifiability //Proceedings of the Australasian Conference on Information Security and Privacy. Cham, Cambodia: Springer, 2016, 9723: 120-133

[36] Zhan Y, Wang B, Wang Z, et al. Improved proxy re-encryption with delegatable verifiability. IEEE Systems Journal, 2019, 14(1): 592-602

[37] Cheng Z. Security analysis of SM9 key agreement and encryption//Proceedings of the International Conference on Information Security and Cryptology. Cham: Springer, 2019, 11449: 3-25

[38] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. Security analysis of SM9 digital signature and key encapsulation. SCIENTIA SINICA Informationis, 2021, 51(11): 1900-1913(in Chinese)
(赖建昌, 黄欣沂, 何德彪等. 国密 SM9 数字签名和密钥封装算法的安全性分析. 中国科学:信息科学, 2021, 51(11): 1900-1913)

[39] Zhen P, Hu X, Yu Y, et al. Research on the optimization computation of SM9 bilinear pairings//Proceedings of the International Conference on Communication and Information Systems. New York, USA, 2017: 256-261

[40] Hu Xin-Yi, He De-Biao, Peng Cong, et al. A fast implementation of R-ate pairing in SM9 algorithm. Journal of Cryptologic Research, 2022, 9(5): 936-948(in Chinese)
(胡芯忆, 何德彪, 彭聪等. 一种 SM9 算法 R-ate 对的快速实现方法. 密码学报, 2022, 9(5): 936-948)

[41] Zhu Liu-Fu, Li Ji-Guo, Lai Jian-Chang, et al. Attribute-based online/offline signature scheme based on SM9. Journal of Computer Research and Development, 2023, 60(2): 362-370(in Chinese)
(朱留富, 李继国, 赖建昌等. 基于商密 SM9 的属性基在线/离线签名方案. 计算机研究与发展, 2023, 60(2): 362-370)

[42] Peng Cong, He De-Biao, Luo Min, et al. An identity-based ring signature scheme for SM9 algorithm. Journal of Cryptologic Research, 2021, 8(4): 724-734(in Chinese)
(彭聪, 何德彪, 罗敏等. 基于 SM9 标识密码算法的环签名方案. 密码学报, 2021, 8(4): 724-734)

[43] An Hao-Yang, He De-Biao, Bao Zi-Jian, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection. Journal of Computer Research and Development, 2023, 60(11): 2545-2554(in Chinese)

(安浩杨，何德彪，包子健等. 基于 SM9 数字签名的环签名及其在区块链隐私保护中的应用. 计算机研究与发展，2023，60(11)：2545-2554)

[44] Qin Bao-Dong, Zhang Bo-Xin, Bai Xue, et al. Mediated SM9 identity-based encryption algorithm. Chinese Journal of Computers, 2022, 45(2): 412-426(in Chinese)
(秦宝东，张博鑫，白雪等. 基于仲裁的 SM9 标识加密算法. 计算机学报，2022，45(2)：412-426)

[45] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. Efficient hierarchical identity-based encryption based on SM9. SCIENTIA SINICA Informationis, 2023, 53(5): 918-930(in Chinese)
(赖建昌，黄欣沂，何德彪等. 基于商用密码 SM9 的高效分层标识加密. 中国科学:信息科学，2023，53(5)：918-930)

[46] Liu Kuan, Ning Jian-Ting, Wu Wei, et al. Multi-ciphertext batch auditable outsourced SM9-HIBE key encapsulation mechanism. Journal o Communications, 2023, 44(12): 158-170(in Chinese)
(刘宽，宁建廷，伍玮等. 支持多密文批量审计的解密外包 SM9-HIBE 密钥封装机制. 通信学报，2023，44(12)：158-170)

[47] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. An efficient identity-based signcryption scheme based on SM9. Journal of Cryptologic Research, 2021, 8(2): 314-329(in Chinese)
(赖建昌，黄欣沂，何德彪等. 基于商密 SM9 的高效标识签密. 密码学报，2021，8(2)：314-329)

[48] Xiong Hu, Lin Ye, Yao Ting. SM9 identity-based encryption scheme with equality test and cryptographic reverse firewalls. Journal of Computer Research and Development, 2024, 61(4): 1070-1084(in Chinese)
(熊虎，林烨，姚婷. 支持等式测试及密码逆向防火墙的 SM9 标识加密方案. 计算机研究与发展，2024，61(4)：1070-1084)

[49] Rackoff C, Simon D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack//Proceedings of the Advances in Cryptology-CRYPTO'91. Berlin, Germany: Springer, 1991, 576: 433-444

[50] Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups. Journal of Cryptology, 2008, 21(2): 149-177

[51] Damgård I B. Collision free hash functions and public key signature schemes//Proceedings of the Advances in Cryptology-EUROCRYPT'87. Berlin, Germany: Springer, 1987, 306: 203-216

LIU Hang, Ph. D. candidate. His research interests include public key cryptography and data sharing security.

MING Yang, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

WANG Chen-Hao, Ph. D. candidate. His research interests include public key cryptography and digital twin security.

ZHAO Yi, Ph. D., lecturer. His research interests include cryptography and network security.

Background

Proxy re-encryption (PRE) technology has been widely applied to secure data sharing in cloud storage thanks to the support of efficient ciphertext transformation. Subsequently, to solve the certificate management problems, Green et al. proposed identity-based PRE (IBPRE). However, PRE and IBPRE only support one-to-one data sharing, which is less flexible in multi-user scenarios. Therefore, Xu et al. introduced the notion of identity-based broadcast PRE (IBBPRE), enabling the data owner share the data with a set of authorized users. All of the above primitives assume that the proxy performs the ciphertext transformation operation honestly, however, in practice, it is very likely that the proxy will return the wrong re-encrypted ciphertext for saving its own computational cost. To eliminate this problem, the verifiable and fair IBBPRE (VF-IBBPRE) schemes are put forward, making the authorized users verify the correctness of re-encrypted ciphertext and the honest proxy be free from malicious accusations. Whereas, the existing schemes have the following problems: additional communication overhead in the verification phase and leakage of the re-encryption key; failure of verifiability caused by the wrong original ciphertext and re-encryption key; and increased computational cost resulting from the generation of additional commitments in the ciphertext.

SM9 identity-based cryptography realizes the national strategic demand for independent control of core technologies, and havs become national standards and ISO/IEC international standards. At present, scholars have conducted extensive

extension studies for the SM9 identity-based encryption algorithm. However, existing solutions either do not take into account the demand for one-to-many data sharing or cannot support ciphertext transformation, resulting in poor flexibility.

To cope with the above problems, in this paper, we put forward a VF-IBBPRE scheme based on SM9 identity-based encryption algorithm. The proposed scheme achieves the verifiability and fairness by utilizing the idea of the Fujisaki-Okamoto transformation and devising the efficient zero-knowledge proof protocol. We optimize the formal definition and security model for VF-IBBPRE to better meet real-world requirements. The security proof demonstrates that our scheme satisfies the indistinguishability against selective identity and chosen plaintext attack, secret key leakage resistance against collusion attack, verifiability, and fairness. Theoretical and experimental analysis show that the proposed scheme obtains advantages in terms of computation and storage costs. Specifically, compared with the related schemes, when the number of authorized users is 20, the computation cost of algorithm Re-KeyGen of the proposed scheme reduces by at least about 59.51%; the computation cost of algorithm DecVerify of the proposed scheme reaches a reduction of at least about 22.27%. At the same time, the proposed scheme offers the lowest storage cost compared to others schemes. Therefore, the proposed scheme is more suitable for multi-user data sharing scenarios.

This work was supported by the National Natural Science Foundation of China under Grant Nos. 62472049 and 62072054, the Key Research and Development Program of Shaanxi Province under Grant No. 2024GX-YBXM-078, the Xi'an Science and Technology Planning Program under Grant No. 23ZDCYJSGG0009-2022 and the Fundamental Research Funds for the Central Universities, CHD, under Grant No. 300102242201.