基于国密算法SM9的撤销加密方案

谢振杰[1,2]，张万里[1]，张耀[1,3]，赵方方[1]，刘胜利[1]

（1.信息工程大学网络空间安全教育部重点实验室，河南 郑州 450001；2.中国人民解放军78156部队，重庆 400039；
3.中国人民解放军新疆昌吉军分区，新疆 昌吉 831100）

摘　要：针对现有标识撤销加密方案存在的系统公钥冗长和解密效率低的问题，基于我国自主研发的标识密码算法SM9，提出一种高效的撤销加密方案。通过在加密阶段指定被撤销用户名单，被撤销用户无法解密，而系统内其余用户均可正常解密。方案实现了恒定长度的密文和精简的系统公钥，针对撤销加密“一次加密、多次解密”的应用场景，通过重构双线性对运算优化了解密效率。在随机预言机模型下，基于广义判定性Diffie-Hellman指数（GDDHE）困难问题证明了方案的选择明文安全性。理论分析和实验测试表明，相较于现有同类方案，所提方案以密钥封装密文长度扩张50%为代价，系统公钥长度缩减约66.7%，当撤销用户数量在4～64个时，解密效率提升65.0%～85.2%。结果表明，所提方案有效增强了SM9密码体系在大规模访问控制场景中的实用性。

关键词：撤销加密；国密算法；SM9算法；广播加密；基于标识的密码

中图分类号：TP309.7

文献标志码：A

DOI：10.11959/j.issn.1000−436x.2025088

Revocation encryption scheme based on domestic cryptographic algorithm SM9

XIE Zhenjie[1,2], ZHANG Wanli[1], ZHANG Yao[1,3], ZHAO Fangfang[1], LIU Shengli[1]

1. Key Laboratory of Cyberspace Security, Ministry of Education, Information Engineering University, Zhengzhou 450001, China
2. Unit 78156 of the Chinese People’s Liberation Army, Chongqing 400039, China
3. Xinjiang Changji Military Subarea of the Chinese People’s Liberation Army, Changji 831100, China

Abstract: To address the limitations of lengthy system public keys and inefficient decryption in existing identity-based revocation encryption schemes, an optimized revocation encryption scheme was proposed based on SM9, China’s independently developed identity-based cryptographic algorithm. During encryption, a revoked user list was specified, ensuring that only non-revoked users could decrypt correctly. The scheme achieved constant ciphertext length and compact system public keys. For the “one-time encryption, multiple decryption” scenario, decryption efficiency was prioritized through bilinear map restructuring. Under the random oracle model, the scheme was proven to achieve chosen-plaintext security based on the GDDHE assumption. Theoretical analysis and experimental tests demonstrated that, compared with existing schemes, the system public key length was reduced by approximately 66.7% at the cost of a 50% expansion in key-encapsulated ciphertext length. When revoking 4 to 64 users, the decryption efficiency was improved by 65.0% to 85.2%. These results indicate that the scheme effectively enhances the practicality of SM9-based cryptographic systems in large-scale access control scenarios.

Keywords: revocation encryption, domestic cryptographic algorithm, SM9 algorithm, broadcast encryption, identity-based cryptography

收稿日期：2025−03−10；修回日期：2025−04−30

通信作者：赵方方，fangfangzhaowlc@163.com

0 引言

广播加密允许数据所有者通过公开信道与多个用户实现数据安全共享[1]，广泛应用于数字版权保护、云计算、区块链及在线会议等场景。在广播加密中，加密者需指定一个接收者集合，仅集合内的用户可正确解密，集合外的用户无法获取明文的任何信息，并且能够防御集合外用户的合谋攻击[2]。然而，由于广播加密需指定全部接收者，其开销与接收者数量呈正相关，当接收者规模庞大时，广播加密将面临效率低下的问题。在相当多的场景下，系统内的用户默认具有解密权限，仅需限制少数用户的权限，例如订阅了付费内容的用户不再续费、用户私钥泄露、用户主动放弃解密权限等。为了能在上述情形下安全高效地共享数据，研究人员提出了撤销加密的概念[3]，作为广播加密的反向应用和补充，它也被视为一种特殊的广播加密类型。撤销加密指定的不是接收者，而是被撤销解密权限的用户集合，仅集合外的用户可正确解密。撤销加密的安全性在于，即使集合内的用户合谋，也无法获取明文的任何信息。当系统内具有访问权限的用户多于被禁止的用户时，撤销加密的效率将高于广播加密。例如，在视频点播服务中，当10%的订阅用户到期未续费时，采用广播加密封装后续密钥需指定90%的续费用户，而撤销加密方案仅需指定10%的撤销名单。

根据加密和解密过程中密钥的不同，广播加密可分为对称广播加密和公钥广播加密[2]。在对称广播加密中，广播者只能是可信机构，应用范围窄。公钥广播加密允许系统内任意用户作为数据拥有者，更具一般性且灵活。传统的公钥密码通常依赖公钥基础设施（PKI, public key infrastructure），通过证书绑定公钥和特定用户的联系，但PKI的建设和运维成本不菲，且证书的申请、验证和管理易导致系统性能瓶颈。在基于标识的密码（IBC, identity-based cryptography）体系下，公钥的验证不依赖证书，而是以能唯一标识用户身份的邮箱、手机号、证件号等字符串作为公钥。IBC一定程度上避免了对第三方机构的依赖，是一类具有广阔应用前景的公钥密码。国密算法SM9是我国自主研发的标识密码，涵盖了数字签名算法、密钥交换协议、密钥封装机制和加密算法[4-5]。SM9基于椭圆曲线构造，除了具备IBC的优势，相比RSA（Rivest-Shamir-Adleman）等传统公钥密码算法，在提供同等安全强度的同时，所需的密钥长度更短，计算效率更高，有利于增强系统的整体安全性和性能。近年来，基于SM9算法设计的密码方案不断扩展，包括同态加密[6-7]、环签名[8-10]、签密[11]、可搜索加密[12]、分层标识加密[13-15]、广播加密[15-18]和容错加密[19]等领域的方案相继问世，展示了SM9出色的性能以及在各种密码应用领域的拓展潜力，有助于提升关键网信基础设施的安全性和自主可控能力。然而，基于SM9的广播加密方案不适用于系统中接收者众多、仅屏蔽少数用户的情况，此时需从撤销加密的角度设计更高效的广播方案。

本文基于国密算法SM9的加密算法，设计了一种基于标识的撤销加密方案。相较于广播加密需指定接收者集合，撤销加密方案在加解密时输入的是被撤销用户的集合，该集合内的用户不具有解密权限（即使合谋也无法解密），而集合外的系统合法用户均可正常解密，无须再额外指定。方案的系统公钥长度与可撤销的最大用户数量线性相关，而用户私钥和封装密文是定长的。基于一个广义的判定性Diffie-Hellman困难问题，在随机预言机模型下，证明了方案能抵抗选择明文攻击（CPA, chosen-plaintext attack）。通过理论分析和实验测试，相较于现有同类方案，本文方案的主要优势在于解密算法优化（双线性对减少$\frac{1}{3}$）和系统公钥精简（缩减约$\frac{2}{3}$）。本文通过重构双线性对运算和调整公钥结构有效降低了广大解密用户的计算和存储开销，提升了国密撤销加密方案的性能和实用性。

1 相关工作

广播加密和撤销加密都是实现多用户数据安全共享的加密技术，广播加密概念提出的时间较早，由Fiat等[1]首次提出，并提供了具体的构造方法。Delerablée[20]研究了IBC体制的广播加密，通过公钥聚合技术，实现了定长的密钥和密文，在随机预言机模型下，证明了所提标识广播加密方案的安全性。Sakai等[21]提出了一个近似的标识广播加密方案。赖建昌等[16]首次将国密算法SM9密钥封装与广播加密相结合，提出了首个基于SM9的标识广播加密方案。赖建昌等[17]基于SM9进一步设计了

具有选择密文安全的广播加密方案。崔岩等[18]提出了一个基于SM9的匿名广播加密方案。文献[2]对各类公钥广播加密的原理、特性以及近年来的代表性成果进行综述，将撤销加密称为接收者可撤销广播加密，视为广播加密的一种类型。由于撤销加密的构造方法与广播加密有近似之处，研究广播加密的最新成果，对于设计撤销加密方案有重要的借鉴意义。

Lewko等[3]首次提出标识撤销加密方案，方案的用户私钥和系统公钥是定长的，但密文长度与撤销的用户数量线性相关。Attrapadung等[22]提出的标识撤销加密方案具有定长密文，但其系统公开参数和用户私钥长度都与可撤销的最大用户数量线性相关。Chen等[23]利用素数阶双线性群提出了一个非零内积加密方案，并在此基础上提出了密文和用户私钥均为定长的撤销加密方案，仅有系统公开参数与可撤销的最大用户数量线性相关。Jiang等[24]提出了一个标识撤销加密方案，采用逆指数技术实现定长的密文和用户私钥，可撤销的最大用户数量是可变的且与系统公开参数线性相关。上述采用国际密码算法实现的标识撤销加密方案继承了对应标识广播加密方案的设计思路和性能，逐步实现了密文长度、公私钥规模与计算开销的平衡，为此类方案设计提供了典型范式，但计算效率仍有优化空间。

Boldyreva等[25]提出的标识加密方案运用密钥更新的方式实现撤销，撤销用户列表定期更新后，由密钥生成中心（KGC, key generation center）广播密钥更新信息，某周期内被撤销的用户无法生成该周期内密文的解密密钥。文献[26-27]进一步研究了通过密钥更新实现撤销的标识加密技术，此路线的优势在于当撤销用户数量大时性能较好，但其撤销用户列表是全局的、周期性的，不利于实现逐密文指定撤销用户集的细粒度撤销。Susilo等[28]提出的标识广播加密方案通过密文更新的方式撤销部分用户的解密权限，该方案允许不知道明文数据的第三方处理密文，被撤销的用户即使在加密阶段指定的接收者集合中，也不能正确解密更新后的密文。Lai等[29]在其基础上进一步实现了撤销集合中用户身份的匿名性，但此类方案的目标是对已经广播的密文进行部分用户撤销，被撤销的用户仍有可能通过原始密文解密。Chen等[30]提出的标识撤销加密方案通过云服务器实现密文更新，解决了用户撤销后仍能访问历史密文的问题，具有恒定大小的密文并实现了选择密文安全，优化了计算和通信效率。Kim[31]提出一种后向兼容的标识撤销加密方案，以解决密钥更新导致历史密文无法解密的问题，其支持将密文更新安全外包至云服务器，简化了密钥管理并适用于物联网等动态环境。上述文献依托第三方处理密文实现灵活撤销，此类方案需权衡好历史密文访问控制与计算效率。

赖建昌等[32]在国内外广播/撤销加密最新研究成果的基础上，基于SM9提出了一个撤销加密方案，方案在加密阶段指定被撤销的用户集合，具有定长的用户私钥和密文，系统公钥长度与可撤销的最大用户数量线性相关，继承了文献[24]方案的设计思路并融入国密算法。该文在随机预言机模型下基于广义的判定性Diffie-Hellman困难问题证明了方案的CPA安全性，通过理论分析和对比，其计算和存储开销与国内外文献中的代表性广播/撤销加密方案相当。

2　基于标识的撤销加密概述

本节列出本文的主要符号含义，分析基于标识的撤销加密方案依赖的数学困难问题，并描述该类方案的典型系统模型和安全模型。

2.1　符号含义

本文的符号含义与SM9国标[4-5]基本一致。表1列出了本文使用的主要符号及其含义，其余符号在首次出现时定义。

表1　主要符号含义

符号	含义
G_1	椭圆曲线加法循环群
G_2	椭圆曲线加法循环群
P_1	G_1的生成元
P_2	G_2的生成元
G_T	乘法循环群
N	大素数，群G_1、G_2、G_T的阶
e	双线性对：$G_1\times G_2\rightarrow G_T$
$[k]U$	椭圆曲线点U的k倍（标量乘）
$x\Vert y$	x与y的字节串拼接
H_1	哈希函数：$\{0,1\}^*\rightarrow Z^*_N$

为简化符号并与方案公开参数P_1、P_2有所区分，在困难问题的实例中，也使用P、Q表示群G_1、G_2的生成元。

2.2　困难问题

令m是不小于2的整数，$f(x)$是$Z_N[x]$中次数为m且有m个不同根的多项式，则在非对称双线性群上定义的一个广义判定性Diffie-Hellman指数（GDDHE, general decision Diffie-Hellman exponent）问题如下。

定义1　(m,f)-GDDHE问题。对于未知的正整数$a, b, c\in[1, N-1]$，给定下列$G_1^{2m+3}\times G_2^{m+2}$元素为

$$\begin{cases}P,[a]P,[f^2(a)bc]P\\ [f(a)b]P,[af(a)b]P,\cdots,[a^m f(a)b]P\\ [ab]P,[a^2b]P,\cdots,[a^{m-1}b]P\\ Q,[a]Q,\cdots,[a^m]Q,[f(a)c]Q\end{cases}$$

以及$T\in G_T$，判断$T=e(P,Q)^{a^m f(a)bc}$是否成立。

若在多项式时间内解决(m,f)-GDDHE问题的优势是可忽略的，则称(m,f)-GDDHE问题的困难性假设成立。

定理1　在通用群模型中，(m,f)-GDDHE问题是困难的。

证明　根据文献[33]的证明思路，首先将问题简化至对称群内。不妨设$G_1=G_2$且$Q=[\beta]P$，(m,f)-GDDHE问题的实例可简化为

$$\boldsymbol{X}=\begin{pmatrix}1,a,f^2(a)bc,\\ f(a)b,af(a)b,\cdots,a^m f(a)b,\\ ab,a^2b,\cdots,a^{m-1}b,\\ \beta,\beta a,\cdots,\beta a^m,\beta f(a)c\end{pmatrix}$$

$$Y=1$$

$$F=\beta a^m f(a)bc$$

再将证明(m,f)-GDDHE问题的困难性转化为证明F与$(\boldsymbol{X},Y)$线性无关，即不存在系数$x_{i,j}$和y满足

$$F=\sum x_{i,j}d_i d_j+y \tag{1}$$

其中，$d_i, d_j\in\boldsymbol{X}$。

为满足式(1)，$\boldsymbol{X}$中元素d_i和d_j的乘积须包含βbc，所有可能的乘积集合如下。

$$\boldsymbol{X}'=\begin{pmatrix}\beta af(a)bc,\beta a^2 f(a)bc,\cdots,\beta a^{m-1}f(a)bc,\\ \beta f^2(a)bc,\beta af^2(a)bc,\cdots,\beta a^m f^2(a)bc\end{pmatrix}=$$

$$\begin{pmatrix}a,a^2,\cdots,a^{m-1},\\ f(a),af(a),\cdots,a^m f(a)\end{pmatrix}\beta f(a)bc$$

然后转化为证明F不是$\boldsymbol{X}'$中元素的线性组合。设$p(a)$和$q(a)$都是关于a的多项式，$p(a)$的次数为1～$m-1$，$q(a)$的次数为0～m，令$p(a)=\sum_{i=1}^{m-1}r_i a^i$，$q(a)=\sum_{i=0}^{m}s_i a^i$，则$\boldsymbol{X}'$中元素的线性组合可表示为$(p(a)+q(a)f(a))\beta f(a)bc$。假设

$$(p(a)+q(a)f(a))\beta f(a)bc=F=\beta a^m f(a)bc \tag{2}$$

成立，式(2)两边消去$\beta f(a)bc$后得

$$p(a)+q(a)f(a)=a^m \tag{3}$$

又$f(a)$的次数为m，令$f(a)=\sum_{i=0}^{m}t_i a^i$，且$t_m\neq 0$；当$a=0$时，有$p(a)=0$，则式(3)左边$=s_0t_0=$式(3)右边$=0$，又$t_0$不恒为0（$f$由问题实例给定，而$p$、$q$可根据需要构造），则$s_0=0$，再分以下2种情况讨论。

1)$s_1, s_2, \cdots, s_m$均为0，即$q(a)$恒为0，此时式(3)左边$=p(a)$，最高次数为$m-1$，而式(3)右边次数为m，这与式(3)成立的假设相矛盾。

2)$s_1, s_2, \cdots, s_m$不全为0，不妨设$s_1\neq 0$而$s_2, \cdots, s_m$均为0，此时式(3)左边$=p(a)+s_1af(a)$，次数为$m+1$，同样与式(3)成立的假设相矛盾。

故F不可能是$\boldsymbol{X}'$中元素的线性组合。因此，(m,f)-GDDHE问题是困难的。证毕。

2.3　系统模型

一个典型的基于标识的撤销加密方案，通常由系统建立Setup、用户加密私钥生成KeyGen、加密Encrypt和解密Decrypt这4项算法构成。KGC运行Setup算法完成系统初始化，运行KeyGen算法为用户生成加密私钥，加密者和解密者分别运行Encrypt和Decrypt算法。其系统模型如图1所示。

1) 系统建立Setup(λ, m)→(**params**, **msk**)：由KGC运行的概率多项式时间（PPT, probabilistic polynomial time）算法，输入安全参数λ和可撤销的最大用户数量m，输出系统公开参数**params**和加密主私钥**msk**。

以下算法的输入都包含**params**，为简化描述不再额外标注。

2) 用户加密私钥生成KeyGen(ID, **msk**)→**sk**：由KGC运行的确定性算法，输入用户身份标识ID和加密主私钥**msk**，输出用户加密私钥**sk**。

3) 加密Encrypt(M, R)→**RC**：由加密者运行的PPT算法，输入待加密消息M和撤销用户集合R，

输出密文**RC**。

4)解密 Decrypt(**RC**, R, ID, **sk**)→M/⊥：由解密者运行的确定性算法，输入密文**RC**、撤销用户集合R、解密者标识ID和私钥**sk**，若ID∉R且解密成功则输出被加密消息M，否则输出⊥（表示解密失败）。

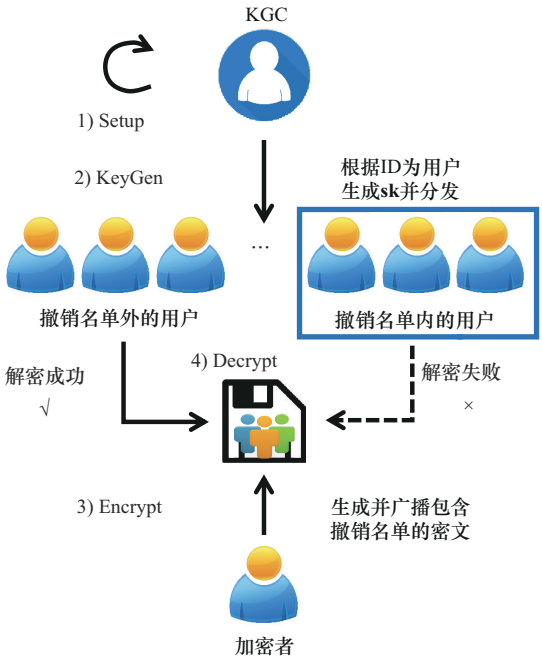


图1　基于标识的撤销加密方案的系统模型

方案的正确性要求如下：对于合法的密文，撤销用户集合R之外的解密者成功解密的概率为1；而对于非法的密文或集合R内的用户，成功解密的概率是可忽略的。方案正确性的形式化表述如下。

$$\text{Setup}(\lambda, m) \rightarrow (\textbf{params}, \textbf{msk})$$

$$\text{KeyGen}(\text{ID}, \textbf{msk}) \rightarrow \textbf{sk}$$

$$\text{Encrypt}(M, R) \rightarrow \textbf{RC}$$

$$\text{Decrypt}(\textbf{RC}, R, \text{ID}, \textbf{sk}) \rightarrow \begin{cases} M, & \text{ID} \notin R \\ \perp, & \text{ID} \in R \end{cases}$$

2.4　安全模型

基于标识的撤销加密方案，应满足静态标识选择明文攻击下的不可区分性（IND-sID-CPA, indistinguishability against selective identity chosen-plaintext attack）。

定义 2　IND-sID-CPA。该性质由挑战者C与PPT敌手A之间的游戏来定义，为简化模型采用密钥封装代替加密，游戏过程分为以下5个阶段。

1) 初始化。敌手A输出挑战的撤销用户集合R^*={$\text{ID}_1^*, \text{ID}_2^*, \cdots, \text{ID}_m^*$}。挑战者$C$调用Setup生成系统公开参数**params**和加密主私钥**msk**，将**params**发送给A。

2)询问1。A询问标识ID∈R^*，C调用KeyGen生成对应的用户加密私钥**sk**并返回。A可询问多次，但不能询问集合R之外的私钥。

3)挑战。C调用Encrypt生成挑战密钥K^*和封装密文**RC***，随机选择b∈{0, 1}，设K_b=K^*，在密钥空间内随机生成K_{1-b}，向A返回挑战密文(**RC***, K_0, K_1)。

4)询问2。A可继续询问标识ID∈R^*的私钥。

5)猜测。A输出b'∈{0, 1}，如果b'=b，则A赢得游戏。

定义A赢得该游戏的优势为 $\text{Adv}_A^{\text{IND-sID-CPA}} = \left| \Pr[b' = b] - \frac{1}{2} \right|$。如果对于任意PPT敌手$A$，该优势是可以忽略的，则称该撤销加密方案IND-sID-CPA是安全的。

3　基于SM9的撤销加密方案构造

本节详细阐述所设计的撤销加密方案的各项算法。由于本文关注的是公钥密码，加解密部分重点描述密钥封装和解封装过程，省略了对称密码算法。

3.1　系统建立Setup

由KGC产生随机数α, β, γ∈[1, N−1]作为加密主私钥，计算群G_1中的元素序列P_{pub}={[γ]P_1, [$\gamma\alpha$]P_1, [$\gamma\alpha^2$]P_1, …, [$\gamma\alpha^m$]P_1}作为加密主公钥，其中m是可撤销的最大用户数量，再计算群G_T中的元素g=e([$\alpha\beta$]P_1, P_2)。加密主密钥为($\alpha, \beta, \gamma, P_{\text{pub}}, g$)，KGC秘密保存$\alpha$、$\beta$、$\gamma$，公开$P_{\text{pub}}$、$g$。KGC选择并公开大小为1B的加密私钥生成函数识别符hid。

3.2　用户加密私钥生成KeyGen

设用户的标识为ID，为产生其加密私钥**sk**，KGC首先计算整数v=H_1(ID ‖ hid, N)，若v+α=0则需重新产生系统加密主密钥，并更新已有用户的加密私钥；否则计算 $d_1 = \left[\frac{\alpha}{v+\alpha}\right]P_2, d_2 = \left[\alpha\beta + \frac{\alpha\gamma}{v+\alpha}\right]P_1$，最后将加密私钥元组**sk**=($d_1$, d_2)通过安全途径传递给用户。

3.3　加密算法Encrypt

设撤销用户集合R={$\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n$}（$n$≤$m$），

待加密的消息为比特串M，加密者生成加密消息**RC**的运算步骤如下。

1)产生随机数$r\in[1, N-1]$，计算群G_T中的元素$\omega=g^r$。

2)计算群G_2中的元素$C_1=[r]P_2$。

3)计算整数$v_i=H_1(\mathrm{ID}_i \| \mathrm{hid}, N)$（$1\leqslant i\leqslant n$），计算群$G_1$中的元素$C_2=\left[r\gamma\prod_{i=1}^{n}(v_i+\alpha)\right]P_1$。

4)计算$K=\mathrm{KDF}(C_1 \| C_2 \| \omega \| R, \mathrm{klen})$。

5)输出加密消息**RC**$=(C_1, C_2)$。

其中，步骤4)中的KDF表示密钥派生函数（key derivation function），整数klen表示密钥的比特数，K为封装好的密钥。

3.4 解密算法Decrypt

设解密者D的标识为ID_D，根据撤销用户集合R（$\mathrm{ID}_\mathrm{D}\notin R$）定义如下多项式

$$f(x)=\frac{\prod_{i=1}^{n}(v_i+x)}{v_\mathrm{D}+x}=\frac{\prod_{i=1}^{n}(v_i-v_\mathrm{D}+v_\mathrm{D}+x)}{v_\mathrm{D}+x}=$$

$$x^{n-1}+t_{n-2}x^{n-2}+\cdots+t_1x+t_0+\frac{z}{v_\mathrm{D}+x}\bmod N$$

其中，$v_\mathrm{D}=H_1(\mathrm{ID}_\mathrm{D} \| \mathrm{hid}, N)$，$t_i$（$0\leqslant i\leqslant n-2$）是可计算的模$N$多项式系数，$z=\prod_{i=1}^{n}(v_i-v_\mathrm{D})\bmod N$。D收到加密消息**RC**$'=(C_1', C_2')$后，运算步骤如下。

1)检验$C_1'\in G_2$和$C_2'\in G_1$是否均成立，若不完全成立则解密失败。

2)计算整数$v_i=H_1(\mathrm{ID}_i \| \mathrm{hid}, N)$（$1\leqslant i\leqslant n$），计算多项式$f(x)$的系数$t_i$（$0\leqslant i\leqslant n-2$）和$z$。

3)计算群G_T中的元素

$$\omega'=e\left(\left[\frac{\gamma(\alpha^n+t_{n-2}\alpha^{n-1}+\cdots+t_1\alpha^2+t_0\alpha)}{z}\right]P_1+d_{2\mathrm{D}}, C_1'\right)e\left(\left[-\frac{1}{z}\right]C_2', d_{1\mathrm{D}}\right)$$

4)计算$K'=\mathrm{KDF}(C_1' \| C_2' \| \omega' \| R, \mathrm{klen})$。

4 方案性质推导与证明

本节通过理论推导，证明本文撤销加密方案的正确性和机密性。

4.1 正确性

如果加密者和解密者诚实地执行上述运算步骤，解密者D不属于撤销用户集合R，且加密消息**RC**在传输过程中未被篡改（即$C_1=C_1'$, $C_2=C_2'$），则方案的正确性来自以下推导。

$$\omega'=e\left(\left[\frac{\gamma(\alpha^n+t_{n-2}\alpha^{n-1}+\cdots+t_1\alpha^2+t_0\alpha)}{z}\right]P_1+d_{2\mathrm{D}}, C_1'\right)e\left(\left[-\frac{1}{z}\right]C_2', d_{1\mathrm{D}}\right)=$$

$$e\left(\left[\frac{\gamma(\alpha^n+t_{n-2}\alpha^{n-1}+\cdots+t_1\alpha^2+t_0\alpha)}{z}\right]P_1+\left[\alpha\beta+\frac{\alpha\gamma}{v_\mathrm{D}+\alpha}\right]P_1, [r]P_2\right)\cdot$$

$$e\left(\left[-\frac{r\gamma\prod_{i=1}^{n}(v_i+\alpha)}{z}\right]P_1, \left[\frac{\alpha}{v_\mathrm{D}+\alpha}\right]P_2\right)=$$

$$e\left(\left[\frac{\alpha\gamma}{z}\left(\alpha^{n-1}+t_{n-2}\alpha^{n-2}+\cdots+t_1\alpha+t_0+\frac{z}{v_\mathrm{D}+\alpha}\right)+\alpha\beta\right]P_1, [r]P_2\right)\cdot$$

$$e\left(\left[\frac{\alpha\gamma}{z}\frac{-r\prod_{i=1}^{n}(v_i+\alpha)}{v_\mathrm{D}+\alpha}\right]P_1, P_2\right)=e\left(\left[\frac{\alpha\gamma r}{z}\big(f(\alpha)-f(\alpha)\big)+\alpha\beta r\right]P_1, P_2\right)=g^r=\omega$$

由$\omega'=\omega$可得，$K'=\mathrm{KDF}(C_1' \| C_2' \| \omega' \| R, \mathrm{klen})=\mathrm{KDF}(C_1 \| C_2 \| \omega \| R, \mathrm{klen})=K$。方案的正确性得证。

此外，若$\mathrm{ID}_\mathrm{D}\in R$，D在解密步骤3)无法消去$d_{2\mathrm{D}}$带来的$\frac{\alpha\gamma}{v_\mathrm{D}+\alpha}$，不能生成正确的$\omega'$，所以无法解密。

4.2 机密性

通过形式化的安全规约方法，在IND-sID-CPA

安全模型下证明所提撤销加密方案的机密性。

定理2　假设哈希函数H_1和密钥派生函数KDF是随机预言机，如果(m,f)-GDDHE问题是困难的，则本文方案在IND-sID-CPA安全模型下是安全的。

证明　假设在IND-sID-CPA安全模型下，存在一个PPT敌手A能以不可忽略的优势ε区分被封装的密钥，则可构建模拟器S解决(m,f)-GDDHE问题。首先，S接收1个(m,f)-GDDHE问题实例，即

$$\begin{cases} P,[a]P,[f^2(a)bc]P \\ [f(a)b]P,[af(a)b]P,\cdots,[a^m f(a)b]P \\ [ab]P,[a^2b]P,\cdots,[a^{m-1}b]P \\ Q,[a]Q,\cdots,[a^m]Q,[f(a)c]Q \end{cases}$$

以及群G_T中的元素T，判断T是否等于$e(P,Q)^{a^m f(a)bc}$。其中，$f(x)$是$Z_N[x]$中次数为m的多项式。不妨设$f(x)=\prod_{i=1}^{m}(w_i^*+x)$，$w_1^*,w_2^*,\cdots,w_m^*\in[1,N-1]$是$m$个互不相同的数。令$f_i(x)=\dfrac{f(x)}{w_i^*+x}=\sum_{j=0}^{m-1}t_j x^j$，$1\leqslant i\leqslant m$，其中，$t_j$（$0\leqslant j\leqslant m-1$）是可计算的多项式系数，且$t_{m-1}=1$。

S以上述实例作为输入，控制随机预言机并运行A的任意攻击算法，进行以下操作。

1)初始化。A指定挑战的撤销用户集合$R^*=\{\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_m^*\}$。$S$随机选择$x\in[1,N-1]$，隐式地设主私钥$\alpha=a,\beta=x-a^{m-1}b,\gamma=f(a)b$，令$P_1=P$，$P_2=[f(a)]Q$，$P_{\mathrm{pub}}=\{[f(a)b]P,[af(a)b]P,\cdots,[a^m f(a)b]P\}$，$g=e([\alpha\beta]P_1,P_2)=e([a(x-a^{m-1}b)]P,[f(a)]Q)=e([xa]P,[f(a)]Q)\cdot e([a^m f(a)b]P,-Q)$。上述公开参数均可通过问题实例和所选的$x$计算得到。

2)哈希询问。H_1、KDF是由S控制的随机预言机，为方便描述，省略其输入项hid、N、klen。开始询问前，S建立2个列表L_1、L_2分别记录H_1、KDF的询问和应答。A可以在任意阶段向S发起以下哈希询问。

①H_1询问。令第i个H_1询问为ID_i，若L_1中已有ID_i对应项，则S根据L_1的记录来应答。否则，当$\mathrm{ID}_i\in R^*$时，有$\mathrm{ID}_i=\mathrm{ID}_j^*$（$1\leqslant j\leqslant m$），设$H_1(\mathrm{ID}_i)=w_j^*$；当$\mathrm{ID}_i\notin R^*$时，$S$随机选择与$w_1^*,w_2^*,\cdots,w_m^*$均不相同的数$w_i\in[1,N-1]$，设$H_1(\mathrm{ID}_i)=w_i$。$S$将$H_1(\mathrm{ID}_i)$作为该询问的应答，并在$L_1$中记录$(i,\mathrm{ID}_i,H_1(\mathrm{ID}_i))$。

②KDF询问。令第i个KDF询问为$C_{1i}\in G_2$，$C_{2i}\in G_1$，$y_i\in G_T$和用户集合R_i，若L_2中已有其对应项，则S根据L_2的记录来应答。否则，S随机生成$K_i\in\{0,1\}^{\mathrm{klen}}$，将$\mathrm{KDF}(C_{1i}\parallel C_{2i}\parallel y_i\parallel R_i)=K_i$作为该询问的应答，并在$L_2$中记录$(i,C_{1i},C_{2i},y_i,R_i,K_i)$。

3)询问1。在此阶段，A可向S询问R^*内标识对应的加密私钥。对于询问对象$\mathrm{ID}_i^*\in R^*$，设$(i^*,\mathrm{ID}_i^*,w_i^*)$为$L_1$中对应的记录（若$L_1$中无此项，则先向$H_1$询问），$S$利用问题实例和$x$计算，即

$$d_{1i}^*=\left[\frac{\alpha}{H_1(\mathrm{ID}_i^*)+\alpha}\right]P_2=\left[\frac{af(a)}{w_i^*+a}\right]Q=[af_i(a)]Q$$

$$d_{2i}^*=\left[\alpha\beta+\frac{\alpha\gamma}{H_1(\mathrm{ID}_i^*)+\alpha}\right]P_1=\left[a(x-a^{m-1}b)+\frac{af(a)b}{w_i^*+a}\right]P=[xa]P+[a(f_i(a)-a^{m-1})b]P$$

可见，$\mathbf{sk}_i^*=(d_{1i}^*,d_{2i}^*)$是一个有效的加密私钥。

4)挑战。A结束询问1后，S令$r^*=c$，利用问题实例和x计算，即

$$C_1^*=[r^*]P_2=[f(a)c]Q$$

$$C_2^*=\left[r^*\gamma\prod_{i=1}^{n}(w_i^*+\alpha)\right]P_1=[cf(a)bf(a)]P=[f^2(a)bc]P$$

$$\omega^*=e([\alpha\beta]P_1,P_2)^{r^*}=e([a(x-a^{m-1}b)]P,[f(a)c]Q)=e([xa]P,[f(a)c]Q)e([-a^m b]P,[f(a)c]Q)=e([xa]P,[f(a)c]Q)T^{-1}$$

$K^*=\mathrm{KDF}(C_1^*\parallel C_2^*\parallel\omega^*\parallel R^*)$

S随机选择$u\in\{0,1\}$，设$K_u=K^*$，随机生成$K_{1-u}\in\{0,1\}^{\mathrm{klen}}$，向$A$发送挑战密文$(C_1^*,C_2^*,K_0,K_1)$。

从以上计算过程可知，当$T=e(P,Q)^{a^m f(a)bc}$时，S利用问题实例模拟的挑战密文与正常加密产生的密文是无法区分的。

5)询问2。A可继续向S发起R^*内标识的私钥询问，S的应答方式同询问1。

6)猜测。A输出猜测结果$u'\in\{0,1\}$。若$u'=u$，S输出$T'=e(P,Q)^{a^m f(a)bc}$；否则，S输出$T'\neq e(P,Q)^{a^m f(a)bc}$。$T'=T$表示$S$猜对该$(m,f)$-GDDHE问题实例。

为推导S破解(m,f)-GDDHE问题的优势，进行如下定义。

$\theta=1$：$T=e(P,Q)^{a^m f(a)bc}$。

$\theta=0$：$T\neq e(P,Q)^{a^m f(a)bc}$。

当$\theta=1$时，理论上能从密文(C_1^*, C_2^*)中解密得到密钥K^*，定义此时A获胜的优势为

$$\mathrm{Adv}_A^{\text{IND-sID-CPA}}=\Pr[u'=u\mid\theta=1]-\frac{1}{2}=\varepsilon$$

当$\theta=0$时，ω^*将成为群G_T中的随机元素，理论上(C_1^*, C_2^*)不能为A求解K^*提供任何依据，故A猜测正确的概率为$\frac{1}{2}$。则S破解(m,f)-GDDHE问题的优势可推导如下。

$$\mathrm{Adv}_S^{(m,f)\text{-GDDHE}}=\Pr[T'=T]-\frac{1}{2}=$$

$$\Pr[u'=u\mid\theta=1]\Pr[\theta=1]+$$

$$\Pr[u'\neq u\mid\theta=0]\Pr[\theta=0]-\frac{1}{2}=$$

$$(\varepsilon+\frac{1}{2})\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}$$

综上，如果存在PPT敌手A能以不可忽略的优势ε区分被封装的密钥，则可以构造模拟器S以不可忽略的优势$\frac{\varepsilon}{2}$破解(m,f)-GDDHE问题，然而这与(m,f)-GDDHE问题的困难性假设相矛盾。因此，本文所提基于SM9的撤销加密方案是IND-sID-CPA安全的。证毕。

5 性能分析与实验

本节对本文方案的计算和通信开销进行理论分析与实验测试，并与符合第2节系统模型的同类代表性成果展开对比。由于各方案的对称加解密细节不尽相同，且不是方案设计关注的重点，下文加密和解密只考虑密钥封装与解封装。

5.1 性能分析

对于计算开销，梳理各撤销加密方案的私钥生成、加密和解密算法中各项耗时运算的次数（可预计算完成的步骤未计入），如表2所示。其中，SM、SM_1、SM_2分别表示对称群G和非对称群G_1、G_2上的标量乘运算，BP表示双线性对运算，E表示群G_T上的幂运算，n表示撤销的用户数。经实测，其余运算（如有限域F_N上的模逆，群G、G_1、G_2上的加法，群G_T上的乘法，以及哈希运算H_1、KDF等）的单次耗时比上述运算低至少低2个数量级，为突出重点已将它们忽略。

本文方案私钥生成和加密的计算量与文献[24]、文献[32]方案基本相同，三者均优于文献[3]方案；相对于文献[32]方案，本文方案的加密过程将1次标量乘从群G_1迁移到群G_2（开销略微增加），而在私钥生成时相反。对于解密算法，本文方案相较于文献[24]、文献[32]方案，通过重构双线性对运算，以增加2次标量乘为代价，消除了1次群G_T上的幂以及1次双线性对，而后两者更耗时（关于双线性群中各项运算的耗时比较可参考文献[34]）。值得注意的是，在文献[24]、文献[32]的解密算法中，均存在输入之一相同的2次双线性对，可等效变换为与本文方案类似的形式（文献[3]解密算法的3次双线性对输入均不相同，无法合并），其中，文献[24]开销降至$(n+1)$SM＋2BP，然而该方案使用对称双线性群，适配国际密码算法，而非SM9所使用的非对称双线性群；文献[32]开销降至$(n+1)\mathrm{SM}_2$＋2BP，但本文方案仍有性能优势，因为本文方案解密只涉及群G_1上的标量乘，其开销约为群G_2标量乘的一半[34]。

对于通信开销，考虑系统公钥、用户私钥和加密消息的比特数（原始消息对应的密文未计入），如表3所示。其中，$|G|$、$|G_1|$、$|G_2|$、$|G_T|$分别表示对应群元素的比特数，m表示可撤销的最大用户数。具体而言，$|G|=512$ bit，对于SM9国标规范使用的256 bit的BN曲线[4]，$|G_1|=512$ bit，$|G_2|=1\,024$ bit，$|G_T|=3\,072$ bit。

可见，只有文献[3]方案的系统公钥长度为常量，但其密文长度与撤销用户数量n线性相关；其余方案的系统公钥长度与可撤销的最大用户数m线

表2 撤销加密方案的计算开销

方案	私钥生成	加密	解密
文献[3]	4SM	$(3n+1)$SM＋E	$2n$SM＋3BP
文献[24]	2SM	$(n+2)$SM＋E	$(n-1)$SM＋E＋3BP
文献[32]	$2\mathrm{SM}_2$	$(n+2)\mathrm{SM}_1$＋E	$(n-1)\mathrm{SM}_2$＋E＋3BP
本文	SM_1＋SM_2	$(n+1)\mathrm{SM}_1$＋SM_2＋E	$(n+1)\mathrm{SM}_1$＋2BP

表3　撤销加密方案的通信开销

方案	系统公钥	用户私钥	加密消息
文献[3]	$\|G_T\|+4\|G\|$	$3\|G\|$	$(2n+1)\|G\|$
文献[24]	$\|G_T\|+(2m+3)\|G\|$	$2\|G\|$	$2\|G\|$
文献[32]	$\|G_T\|+(m+2)\|G_2\|+(m+3)\|G_1\|$	$2\|G_2\|$	$2\|G_1\|$
本文	$\|G_T\|+\|G_2\|+(m+2)\|G_1\|$	$\|G_2\|+\|G_1\|$	$\|G_2\|+\|G_1\|$

性相关，而密文长度为常量。当m较大时，本文方案相较于文献[32]方案，系统公钥长度缩减约$\frac{2}{3}$，密文长度增加$\frac{1}{2}$（增量为64 B，若G_1、G_2上的椭圆曲线点以压缩形式存储，增量为32 B），若考虑原始消息对应的密文通常占据较大份额，密钥封装密文的少量扩张是可接受的。

实际应用中，若系统公钥存储受限（如物联网设备），或解密频次远高于加密（如视频点播服务），本文方案的公钥精简和解密优化更具优势。此外，在安全性方面，上述方案均实现了CPA安全，其中文献[3]方案不依赖于随机预言机模型，而文献[24]、文献[32]和本文都是基于GDDHE困难问题和随机预言机模型，证明了方案具有IND-sID-CPA安全性。

5.2　实验测试

本文基于国密算法开源Python库hggm[35]的SM9模块，使用Python语言编程实现了本文方案和文献[32]方案（包括优化后的解密算法），并引入同样基于SM9且加解密流程相近的广播加密方案[16]作为参考，以验证本文方案的有效性与性能。实验计算机的配置如表4所示。

表4　实验计算机配置

项目	配置
设备类型	PC
操作系统	Windows10 64位
CPU	Intel Core i3-10110U（2核心4线程）
内存	8GB LPDDR3 2133MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python版本	3.7.1

当撤销/广播的用户数量n分别为4、8、16、32、64时，测试加密和解密的单次耗时，结果如表5所示，各撤销加密方案的计算耗时对比如图2所示。可预计算的步骤已提前进行，其耗时不计入。各项算法均执行500次，取平均值为有效数据。

表5　撤销或广播加密方案的加解密耗时

撤销或广播用户数量/个	来源	类型	加密耗时/ms	解密耗时/ms
4	文献[32]	撤销	26.63	111.05
	文献[32]优化	撤销	—	81.43
	本文	撤销	26.61	67.32
	文献[16]	广播	26.87	74.83
8	文献[32]	撤销	43.07	148.24
	文献[32]优化	撤销	—	117.72
	本文	撤销	42.92	87.37
	文献[16]	广播	43.57	95.20
16	文献[32]	撤销	76.62	217.36
	文献[32]优化	撤销	—	186.30
	本文	撤销	77.79	124.12
	文献[16]	广播	78.65	131.51
32	文献[32]	撤销	142.30	336.70
	文献[32]优化	撤销	—	304.92
	本文	撤销	144.13	184.55
	文献[16]	广播	144.05	192.17
64	文献[32]	撤销	278.06	590.49
	文献[32]优化	撤销	—	570.62
	本文	撤销	279.37	318.85
	文献[16]	广播	276.47	324.04

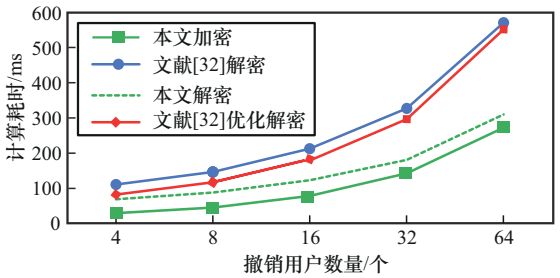


图2　撤销加密方案的计算耗时对比

根据表5数据，各方案加密效率基本一致，本文方案相对文献[32]方案在加密阶段增加的开销极小，难以从测试数据中观测。当用户数量n分别为4、8、16、32、64时，相较于文献[32]方案的解密算法，在其基础上优化可使效率分别提升36.4%、25.9%、16.7%、10.4%、3.5%，由于省去的1次双线性对在总耗时中的占比随n增大而降低，故性能提升幅度逐渐减小；而本文方案解密效率分别提升65.0%、69.7%、75.1%、82.4%、85.2%，可见，将标量乘从群G_2迁移至群G_1的优势随n增大而逐渐扩大。此外，相较于解密时同样在群G_1计算标量乘的广播方案[16]，本文方案仍有性能优势。

综上，本文方案相较于现有同类撤销加密方案，以适当增加密文长度为代价，大幅精简了系统公钥，解密算法性能具有明显优势。

6 结束语

基于标识的撤销加密作为广播加密的补充，在大部分用户为解密者、仅需限制少数用户的情况下，即撤销用户数量少于广播接收者数量时，撤销加密相较于广播加密能显著提高计算效率，应用场景广泛。本文基于国密算法SM9设计了一种高效的撤销加密方案，在随机预言机模型下基于(m, f)-GDDHE困难问题证明其具有IND-sID-CPA安全性，通过理论分析和编程实现验证了解密效率的比较优势。本文方案的撤销方式是在加密时指定被撤销用户名单，使得被撤销用户无法解密。考虑到撤销/广播加密的实际应用场景通常是“一次加密、多次解密”，相较于文献[32]方案，本文方案对于解密算法的优化降低了解密时延，有利于改善用户体验；系统公钥需长期存储，其精简对于物联网设备等资源受限终端是至关重要的；密钥封装密文长度较文献[32]增加$\frac{1}{2}$，但64 B/32 B的增量在大量业务数据（如音视频、文档）中的占比几乎可忽略。总之，本文方案有效提升了基于SM9的撤销加密方案的时空效率和实用性，进一步丰富了国密算法与撤销加密相结合的实践。本文的局限性在于可撤销的最大用户数量与系统公钥长度线性相关，需在系统初始化时预设，难以动态扩展撤销容量，下一步将尝试设计新的用户集合嵌入方式，在进一步精简系统公钥的同时实现撤销容量的弹性扩展。此外，考虑到撤销名单可能涉及隐私，匿名撤销机制也是一个有价值的研究方向。

参考文献：

[1] FIAT A, NAOR M. Broadcast encryption[C]// Advances in Cryptology — CRYPTO’93. Berlin: Springer, 1994: 480-491.

[2] 崔岩, 黄欣沂, 赖建昌, 等. 公钥广播加密研究综述[J]. 广州大学学报(自然科学版), 2022, 21(4): 53-67.
CUI Y, HUANG X Y, LAI J C, et al. A survey on public-key broadcast encryption[J]. Journal of Guangzhou University (Natural Science Edition), 2022, 21(4): 53-67.

[3] LEWKO A, SAHAI A, WATERS B. Revocation systems with very small private keys[C]//Proceedings of the 2010 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2010: 273-285.

[4] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第1部分：总则: GB/T 38635.1—2020[S]. 北京: 中国标准出版社, 2020.
State Administration for Market Regulation, National Standardization Administration. Information security technology-Identity-based cryptographic algorithms SM9: Part 1: General: GB/T 38635.1—2020[S]. Beijing: Standards Press of China, 2020.

[5] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第2部分：算法: GB/T 38635.2—2020[S]. 北京: 中国标准出版社, 2020.
State Administration for Market Regulation, National Standardization Administration. Information security technology-Identity-based cryptographic algorithms SM9: Part 2: Algorithms: GB/T 38635.2—2020[S]. Beijing: Standards Press of China, 2020.

[6] 唐飞, 凌国玮, 单进勇. 基于国密SM2和SM9的加法同态加密方案[J]. 密码学报, 2022, 9(3): 535-549.
TANG F, LING G W, SHAN J Y. Additive homomorphic encryption schemes based on SM2 and SM9[J]. Journal of Cryptologic Research, 2022, 9(3): 535-549.

[7] 秦体红, 汪宗斌, 刘洋, 等. 基于商密SM9算法同态加密方案[J]. 信息安全研究, 2024, 10(6): 513-518.
QIN T H, WANG Z B, LIU Y, et al. Homomorphic encryption scheme based on commercial cryptography SM9[J]. Journal of Information Security Research, 2024, 10(6): 513-518.

[8] 彭聪, 何德彪, 罗敏, 等. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021, 8(4): 724-734.
PENG C, HE D B, LUO M, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.

[9] 饶金涛, 崔喆. 基于SM9盲签名与环签名的安全电子选举协议[J]. 计算机工程, 2023, 49(6): 13-23, 33.
RAO J T, CUI Z. Secure e-voting protocol based on SM9 blind signature and ring signature[J]. Computer Engineering, 2023, 49(6): 13-23, 33.

[10] 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[J]. 计算机研究与发展, 2023, 60(11): 2545-2554.
AN H Y, HE D B, BAO Z J, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection[J]. Journal of Computer Research and Development, 2023, 60(11): 2545-2554.

[11] 赖建昌, 黄欣沂, 何德彪, 等. 基于商密SM9的高效标识签密[J]. 密码学报, 2021, 8(2): 314-329.
LAI J C, HUANG X Y, HE D B, et al. An efficient identity-based signcryption scheme based on SM9[J]. Journal of Cryptologic Research, 2021, 8(2): 314-329.

[12] 蒲浪, 林超, 伍玮, 等. 基于SM9的公钥可搜索加密方案[J]. 信息安全学报, 2023, 8(1): 108-118.
PU L, LIN C, WU W, et al. A public-key encryption with keyword search scheme from SM9[J]. Journal of Cyber Security, 2023, 8(1): 108-118.

[13] 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[J]. 中国科学: 信息科学, 2023, 53(5): 918-930.
LAI J C, HUANG X Y, HE D B, et al. Efficient hierarchical identification encryption based on commercial password SM9[J]. Scientia Sinica (Informationis), 2023, 53(5): 918-930.

[14] 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[J]. 通信学报, 2023, 44(12): 158-170.
LIU K, NING J T, WU W, et al. Multi-ciphertext batch auditable decryption outsourcing SM9-HIBE key encapsulation mechanism[J]. Journal on Communications, 2023, 44(12): 158-170.

[15] 李聪, 梁俊凯, 丁煜甲, 等. 基于SM9的分层标识广播内积函数加密[J]. 中国科学: 信息科学, 2024, 54(6): 1400-1418.
LI C, LIANG J K, DING Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9[J]. Scientia Sinica (Informationis), 2024, 54(6): 1400-1418.

[16] 赖建昌, 黄欣沂, 何德彪. 一种基于SM9的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897-907.
LAI J C, HUANG X Y, HE D B. An efficient identity-based broadcast encryption scheme based on SM9[J]. Chinese Journal of Computers, 2021, 44(5): 897-907.

[17] 赖建昌, 黄欣沂, 何德彪, 等. 基于SM9的CCA安全广播加密方案[J]. 软件学报, 2023, 34(7): 3354-3364.
LAI J C, HUANG X Y, HE D B, et al. CCA secure broadcast encryption based on SM9[J]. Journal of Software, 2023, 34(7): 3354-3364.

[18] 崔岩, 黄欣沂, 赖建昌, 等. 基于SM9的匿名广播加密方案[J]. 信息安全学报, 2023, 8(6): 15-27.
CUI Y, HUANG X Y, LAI J C, et al. Anonymous broadcast encryption based on SM9[J]. Journal of Cyber Security, 2023, 8(6): 15-27.

[19] LIU X H, HUANG X Y, CHENG Z H, et al. Fault-tolerant identity-based encryption from SM9[J]. Science China Information Sciences, 2024, 67(2): 122101.

[20] DELERABLÉE C. Identity-based broadcast encryption with constant size ciphertexts and private keys[C]//2007 International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2007: 200-215.

[21] SAKAI R, FURUKAWA J. Identity-based broadcast encryption[J]. IACR Cryptology ePrint Archive, 2007(217): 1-14.

[22] ATTRAPADUNG N, HERRANZ J, LAGUILLAUMIE F, et al. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical Computer Science, 2012, 422: 15-38.

[23] CHEN J, LIBERT B, RAMANNA S C. Non-zero inner product encryption with short ciphertexts and private keys[C]//2016 International Conference on Security and Cryptography for Networks. Berlin: Springer, 2016: 23-41.

[24] JIANG P, LAI J C, GUO F C, et al. Identity-based revocation system: enhanced security model and scalable bounded IBRs construction with short parameters[J]. Information Sciences, 2019, 472: 35-52.

[25] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008: 417-426.

[26] LI J, LI J W, CHEN X F, et al. Identity-based encryption with outsourced revocation in cloud computing[J]. IEEE Transactions on Computers, 2015, 64(2): 425-437.

[27] GE A J, WEI P W. Identity-based broadcast encryption with efficient revocation[C]//2019 International Conference on Practice and Theory of Public-key Cryptography. Berlin: Springer, 2019: 405-435.

[28] SUSILO W, CHEN R M, GUO F C, et al. Recipient revocable identity-based broadcast encryption[C]//2016 Asia Conference on Computer and Communications Security. New York: ACM Press, 2016: 201-210.

[29] LAI J C, MU Y, GUO F C, et al. Anonymous identity-based broadcast encryption with revocation for file sharing[C]//2016 Australasian Conference on Information Security and Privacy. Berlin: Springer, 2016: 223-239.

[30] CHEN Z W, DENG L Z, RUAN Y, et al. An efficient revocable identity-based encryption with ciphertext evolution in the cloud-assisted system[J]. Concurrency and Computation: Practice and Experience, 2023, 35(22): 1-16.

[31] KIM J. Backward compatible identity-based encryption[J]. Sensors, 2023, 23(9): 1-16.

[32] 赖建昌, 黄欣沂, 何德彪, 等. 基于SM9的撤销加密方案[J]. 软件学报, 2024, 35(12): 5609-5620.
LAI J C, HUANG X Y, HE D B, et al. Revocation encryption scheme based on SM9[J]. Journal of Software, 2024, 35(12): 5609-5620.

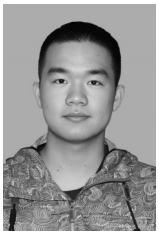
[33] KIM J, SUSILO W, AU M H, et al. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 679-693.

[34] 谢振杰, 刘奕明, 蔡瑞杰, 等. 国密算法SM9的性能优化方法[J]. 计算机科学, 2024, doi: 50.1075.tp.20240823.1457.002.
XIE Z J, LIU Y M, CAI R J, et al. Performance optimization method of domestic cryptographic algorithm SM9[J]. Computer Science, 2024, doi: 50.1075.tp.20240823.1457.002.

[35] 谢振杰, 付伟, 罗芳. 国密算法Python工具包的性能优化方法[J]. 信息安全研究, 2023, 9(10): 1001-1007.
XIE Z J, FU W, LUO F. Performance optimization method of Python toolkit for domestic cryptographic algorithm[J]. Journal of Information Security Research, 2023, 9(10): 1001-1007.

[作者简介]

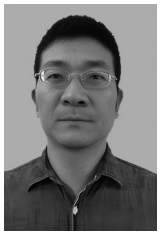
谢振杰（1995– ），男，湖南湘潭人，信息工程大学博士生，主要研究方向为云安全、密码学应用。



张万里（1998– ），男，湖南常德人，信息工程大学博士生，主要研究方向为大数据安全、二进制代码分析。

张耀（1984– ），男，四川自贡人，信息工程大学博士生、工程师，主要研究方向为网络安全、源代码分析、漏洞挖掘。

赵方方（1990– ），女，河南周口人，博士，信息工程大学讲师，主要研究方向为网络安全、网络流量异常检测。



刘胜利（1973– ），男，河南周口人，博士，信息工程大学教授、博士生导师，主要研究方向为网络设备安全、网络攻击检测。