软件学报 ISSN 1000-9825, CODEN RUXUEW
2024,35(12):5609−5620 [doi: 10.13328/j.cnki.jos.007041] [CSTR: 32375.14.jos.007041]

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

基于 SM9 的撤销加密方案*

赖建昌[1], 黄欣沂[2], 何德彪[3], 陈立全[1], 杨少军[4,5]

[1](东南大学 网络空间安全学院, 江苏 南京 211189)

[2](香港科技大学 (广州), 广东 广州 511455)

[3](武汉大学 国家网络安全学院, 湖北 武汉 430073)

[4](福建师范大学 数学与统计学院, 福建 福州 350117)

[5](分析数学及应用教育部重点实验室 (福建师范大学), 福建 福州 350117)

通信作者: 黄欣沂, E-mail: xyhuang81@gmail.com

摘　要: 撤销加密是一种反向的广播加密技术, 加密算法的输入不是接收者集合而是撤销用户的集合, 系统中所有不在撤销集合中的用户都可以正确解密密文, 撤销集合中的所有用户合谋也无法获取加密数据的内容. 与广播加密相比, 撤销加密更适用于接收者为系统中大多数用户或需要撤销部分用户未来解密权限的场景. 基于我国商用标识密码提出一个基于 SM9 的撤销加密方案, 密文的长度是固定的, 与撤销用户集合的大小无关. 基于广义群模型中的困难假设, 证明方案在随机谕言机模型下具有选择明文的安全性. 最后, 分析方案的性能对比结果可知, 所提方案与目前基于身份的撤销加密方案在计算复杂度和存储复杂度方面相比性能相当.

关键词: 撤销加密; SM9; 广播加密; 可证明安全; 定长密文

中图法分类号: TP309

中文引用格式: 赖建昌, 黄欣沂, 何德彪, 陈立全, 杨少军. 基于SM9的撤销加密方案. 软件学报, 2024, 35(12): 5609–5620. http://www.jos.org.cn/1000-9825/7041.htm

英文引用格式: Lai JC, Huang XY, He DB, Chen LQ, Yang SJ. Revocation Encryption Scheme Based on SM9. Ruan Jian Xue Bao/Journal of Software, 2024, 35(12): 5609–5620 (in Chinese). http://www.jos.org.cn/1000-9825/7041.htm

Revocation Encryption Scheme Based on SM9

LAI Jian-Chang[1], HUANG Xin-Yi[2], HE De-Biao[3], CHEN Li-Quan[1], YANG Shao-Jun[4,5]

[1](School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China)

[2](The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511455, China)

[3](School of Cyber Science and Engineering, Wuhan University, Wuhan 430073, China)

[4](School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China)

[5](Key Laboratory of Analytical Mathematics and Applications (Ministry of Education)(Fujian Normal University), Fuzhou 350117, China)

Abstract: Revocation encryption is a negative analogue of broadcast encryption. Unlike broadcast encryption, the input to the encryption algorithm is not a receiver set, but a set of revoked users. All users who are not in the revocation set within the system can decrypt the ciphertext successfully. Users in the revocation set learn nothing about the encrypted data, even in collusion. Compared to broadcast encryption, revocation encryption is more suitable for scenarios where most of the users in the system are the intended recipients and when revoking decryption rights for certain users is required. This study proposes a revocation encryption scheme based on the Chinese identity-based encryption standard SM9. The ciphertext size in the proposed scheme remains constant, and it is independent of the size of the revocation set. Based on a complex assumption in the generic group model, the scheme is proven secure against CPA under the random oracle model. Finally, the performance of the scheme is analyzed, and the results indicate that its computational costs and storage overheads are comparable to the existing revocation encryption schemes.

* 基金项目: 国家自然科学基金 (62032005, U21A20466, U22B2026, 62272104); 东南大学新进教师科研启动项目 (RF1028623200)
收稿时间: 2023-05-15; 修改时间: 2023-06-21; 采用时间: 2023-08-17; jos 在线出版时间: 2024-09-14
CNKI 网络首发时间: 2024-09-18

Key words: revocation encryption; SM9; broadcast encryption; provable security; constant size ciphertext

1 引 言

广播加密[1]是一种在多用户环境中实现数据高效安全共享的技术. 发送者 (加密者) 通过选取一个接收者集合加密数据, 使得只有在集合中的用户才能正确解密. 不在集合中的用户合谋也无法获取加密数据的任何内容. 广播加密允许数据拥有者通过公开信道和多位用户同时安全共享同一数据, 在数字版权、云计算等应用中广泛使用. 标识广播加密[2]不仅继承了广播加密的功能, 而且消除了用于绑定用户身份信息的证书, 任何能够唯一识别用户身份的字符串都可以作为用户的公钥, 用于证明其身份信息, 比如邮箱地址、电话号码等, 极大地节省了用户的计算资源.

由于广播加密中加密算法的开销与接收者的数量线性增长, 因此, 广播加密技术不适用于接收者数量非常大的情况. 特别地, 当系统重接收者的数量远远大于非接收者的数量时, 使用传统的广播加密共享数据效率低下. 此外, 用户的密钥存在需要撤销的情况, 比如在付费电视系统中, 当用户不再付费续租时, 需要撤销相应密钥对后续广播的解密权限. 同时, 用户的密钥也可能遭到泄露, 此时, 同样要求撤销其对未来广播加密密文的解密权限, 以保障数据的隐私. 为了高效解决上述问题, 撤销加密[3]的概念被提出, 在该系统中加密数据的集合不再是接收者的公钥集合, 而是撤销用户的公钥集合. 当且仅当用户不在撤销集合中才能完成正确的解密, 撤销集合内的用户无法获取加密数据的内容. 撤销加密可以看成是反向的广播加密, 是广播加密技术的一种补充, 适用于只有小部分用户不是接收者的应用场景. 在此情况下, 使用撤销加密技术比使用广播加密技术更加高效. 本文侧重于标识撤销加密系统.

自撤销加密技术被提出用于实现用户的撤销或者大范围的广播后, 撤销加密得到了广泛的研究. Lewko 等人[3]提出了具有定长用户私钥和系统公钥的标识撤销加密方案, 但其密文长度与撤销用户的数量成线性增长关系. Attrapadung 等人[4]提出具有定长密文的标识撤销方案, 系统公开参数的长度和用户私钥的长度都与最大撤销用户的数量线性相关. 文献 [5] 基于素数阶双线性群提出了一个非零内积加密 (non-zero inner product encryption) 方案, 并基于该内积加密方案提出了具有定长密文和用户私钥的撤销加密方案, 方案的系统公开参数长度与系统允许撤销用户的最大数量线性相关. Jiang 等人[6]提出了支持改变系统撤销用户最大值的一种标识撤销加密方案.

SM9 是我国自主研发的商用密码, 包括密钥交换协议、公钥加密算法、数字签名算法等系列标识密码, 其中公钥加密算法和数字签名算法现已成为国家标准和国际标准. 自 SM9 标识加密算法被提出后, 已取得了优秀的研究成果[7−12]. 但其设计初衷是为了满足网络和信息系统的共性基础安全需求, 只考虑单接收者场景. 据此, 赖建昌等人[7]把广播加密技术[2]应用于 SM9 标识加密算法, 提出首个基于 SM9 的广播加密方案. 方案具有定长密文, 与接收者数量无关, 并基于随机谕言模型证明了方案满足选择明文的安全性. 随后, 在文献 [8] 中给出了具有选择密文安全的 SM9 广播加密方案. 与现有广播加密一样, 方案不适用于系统中接收者非常大的应用, 特别是系统中只有少数用户不是接收者的情况.

1.1 本文贡献

基于以上分析, 本文采用公钥聚合技术和多项式技术, 提出基于 SM9 的标识撤销加密方案. 加密数据不再使用接收者的标识集合, 而是使用撤销用户的标识集合. 不在集合中的用户属于授权用户, 可以正常解密. 在集合中的用户属于撤销用户, 没有解密权限, 即使共谋也无法解密. 方案具有定长密钥和密文, 系统公钥的长度与一次加密允许撤销的用户最大数量线性相关. 方案在随机谕言机模型下可证明是选择明文攻击 (chosen-plaintext attack, CPA) 安全的. 安全性可归约到一个广义判定性 Diffie-Hellman 困难问题. 最后, 比较本文方案和现有标识广播加密 (identity based broadcase encryption, IBBE) 方案和标识撤销加密方案在计算开销和存储开销方面的性能, 理论分析结果表明, 方案在以上两个方面和现有相关方案表现相当.

一方面, 本文方案可作为文献 [7,8] 的补充, 当数据的接收者为系统中大多数用户时, 采用本文方案共享数据效率比采用文献 [7,8] 的效率高. 在此种情况下, 把非接收者当成撤销用户的列表. 另一方面, 本文方案为 SM9 加密算法在多用户环境下提供了一种用户撤销机制, 当系统中部分用户的密钥泄露后, 可采用本文方案撤销用户密

钥对后续广播的解密权限, 进一步丰富和完善我国商用密码体制.

1.2 相关工作

广播加密[1]是一种实现多用户数据安全共享的加密技术, 它允许数据拥有者 (加密者) 通过公开信道与一组指定的用户安全共享同一数据, 当且仅当用户属于加密时选定的集合就可以正确解密获取数据, 不在集合中的用户即使合谋也无法获取加密数据的内容, 该性质也称为抗合谋攻击. 与重复使用常规的单用户加密技术相比, 广播加密具有效率高的特点. 因此, 广播加密广泛用于付费电视、云计算、物联网等应用中.

Fiat 等人[1]在引入广播加密概念的同时, 提出了首个广播加密的具体构造, 但方案只能抵抗有限个合谋者的攻击. Boneh 等人[13]提出了第 1 个具有定长密钥和密文的抗完全合谋广播加密方案. Gentry 等人[14]给出了在标准模型下具有自适应性安全的方案构造, 但无法实现定长密文. 2007 年, Delerablée[2]研究了标识密码体系中的广播加密, 利用公钥聚合技术提出了具有定长密钥和密文的 IBBE 方案, 并基于随机谕言机模型分析了方案的安全性. 同年, Sakai 等人在文献 [15] 中以独立的工作也提出了一个类似的 IBBE 方案. Kim 等人[16]利用对偶加密技术提出一个在标准模型下具有自适应性安全的定长密文的 IBBE 方案, 但方案中系统公钥和用户私钥的长度与接收者数量线性增长. 文献 [17] 利用虚设标识提出具有静态选择密文安全的 IBBE 方案. 后续广播加密的研究主要是采用文献 [2,13] 中的技术实现不同的安全需求. 具有匿名性的广播加密方案在文献 [18−20] 中得到了进一步的研究, 用户的身份信息不需要和密文一起传输, 有效保障了接收者的隐私.

撤销加密可以看成是反向广播加密, 通过撤销用户或者是非接收者的公钥集合加密数据, 当且仅当用户不在撤销集合中才能正确解密. 基于公钥的撤销加密技术通常分为 4 类. 第 1 类是在群元素的指数上使用插值多项式, 包括方案 [21,22]. 这些方案在系统生成算法阶段选取一个 t 次多项式, 其中 t 为系统允许撤销用户的最大数量, 方案的公开参数和密文与 t 相关. 第 2 类是使用子集覆盖 (subset-cover) 技术. 采用该技术的方案一般基于无状态树形结构设计算法, 包括方案 [23−25]. 此技术还可进一步实现泄露密钥用户的追踪. 第 3 类是采用文献 [26] 提出的逆指数 (exponent-inversion) 技术, 可用于实现定长密文方案的构造[6], 但系统公开参数的长度是线性的. 第 4 类是采用文献 [3] 提出的“two-equation”技术, 用于实现短公钥和短密钥, 但密文长度是线性的. 前面两类技术主要用于传统公钥体制中撤销加密方案的构造, 后面两类技术主要用于标识密码体制中撤销加密方案的设计. 本文采用逆指数技术研究 SM9 密码算法中的撤销加密.

Boldyreva 等人[27]在 2008 年的 CCS 会议上提出了另一种撤销的概念, 通过密钥更新的方法实现用户的撤销. 在标识撤销系统中, 每个用户都有一个永久私钥, 该私钥由 PKG 产生, 用于解密密钥的生成. 每隔一个时间周期 T, PKG 根据撤销用户列表生成并广播用于更新密钥的信息 ku_T , 只有不在撤销列表中的用户才能通过永久私钥和密钥更新信息 ku_T 生成解密密钥 $sk_{(ID,T)}$, 用于解密时间周期 T 内生成的密文. 在撤销列表中的用户则无法通过密钥更新生成相应的解密密钥. 通过密钥更新实现用户解密权限的撤销在文献 [28,29] 得到进一步的研究. 本文的撤销加密方案侧重于利用用户撤销列表生成密文进而实现用户解密权限的撤销.

Susilo 等人[30]提出了撤销标识广播加密密文中部分接收者解密权限的方案. 在该系统中, 第三方可以在不知道加密数据的情况下通过密文更新撤销部分接收者. 如果用户在撤销列表中, 即使属于加密阶段指定的用户集合也无法正确解密. Lai 等人[31]基于文献 [30] 进一步实现了匿名性, 即对撤销集合中用户的身份信息进行保护. 该技术的目的是撤销广播加密密文中部分接收者的解密权限, 和本文研究的撤销加密不同.

SM9 是我国自主研制的身份基 (标识) 密码算法, 自提出后取得了丰富的研究成果[7,9−12,32,33]. Cheng[32]给出了 SM9 加密算法的安全性证明. 赖建昌等人[7]把广播加密技术应用到 SM9 标识加密中, 提出了首个基于 SM9 的广播加密方案, 并在文献 [8] 中进一步地实现了选择密文的安全性. 文献 [10,12] 研究了基于 SM9 的可搜索加密. 唐飞等人[9]提出了基于 SM9 的同态加密算法. 张雪锋等人[11]利用二叉树提出了基于 SM9 的可撤销加密, 用户的撤销通过密钥更新实现. 文献 [33,34] 研究了 SM9 算法中双线性对运算的优化.

1.3 本文组织结构

第 2 节主要给出密码算法构造需要的数学工具, 包括双线性映射和本文方案安全性依赖的困难问题. 标识撤

销加密的形式化定义和相应的安全模型在第 3 节给出. 第 4 节提出 CPA 安全的标识撤销加密方案, 基于安全模型给出方案的安全性证明, 并分析方案的性能. 第 5 节总结本文工作.

2 预备知识

本文方案的构造基于双线性群, 本节首先回顾双线性群的定义和困难问题假设.

2.1 双线性映射

设系统的安全参数为 λ, $\mathbb{G}_1$、 $\mathbb{G}_2$ 和 $\mathbb{G}_T$ 是 3 个阶为 p 的循环群, 其中 p 是由 λ 决定的大素数. 映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 如果满足以下条件则称为双线性映射: (1) 对任意 $g\in\mathbb{G}_1$, $h\in\mathbb{G}_2$ 和 $a,b\in\mathbb{Z}_p$, 都有 $e(g^a,h^b)=e(g,h)^{ab}$; (2) 至少存在元素 $g\in\mathbb{G}_1$, $h\in\mathbb{G}_2$, 满足 $e(g,h)\neq 1$; (3) 对于任意的 $g\in\mathbb{G}_1$, $h\in\mathbb{G}_2$, 存在多项式时间算法高效地计算 $e(g,h)$. 令 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$ 为双线性群. 当 $\mathbb{G}_1=\mathbb{G}_2$ 时, 双线性群为对称双线性群, 否则称为非对称双线性群.

2.2 复杂性假设

方案的安全性基于一个广义判定性 Diffie-Hellman 假设 (general decision Diffie-Hellman exponent assumption, GDDHE), 记为 (m,n,f)-GDDHE 假设. (m,n,f)-GDDHE 问题定义如下: 设 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$ 是与系统安全参数 λ 相关的双线性群, g_0, h_0 分别为群 $\mathbb{G}_1$, $\mathbb{G}_2$ 的生成元. 令 n 和 m 是满足关系 $2\leqslant n\leqslant m$ 的正整数, f 是具有 n 个不同根的 n 阶多项式.

输入: 元素

$$\begin{cases} g_0, g_0^a, g_0^{ar}, g_0^{f(a)^2br}, \\ g_0^{f(a)b}, g_0^{f(a)ba}, g_0^{f(a)ba^2}, \ldots, g_0^{f(a)ba^m}, \\ h_0, h_0^a, h_0^{a^2}, \ldots, h_0^{a^m}, \\ h_0^{f(a)b}, h_0^{f(a)ba}, h_0^{f(a)ba^2}, \ldots, h_0^{f(a)ba^{n-2}}, \\ h_0^{f(a)^2b}, h_0^{f(a)^2ba}, h_0^{f(a)^2ba^2}, \ldots, h_0^{f(a)^2ba^m}, \end{cases}$$

和群 $\mathbb{G}_T$ 中的一个元素 T, 判断 T 是否等于 $e(g_0,h_0)^{a^nf(a)br}$ 或者是群 $\mathbb{G}_T$ 中的一个随机元素, 其中 $a,b,r\in\mathbb{Z}_p$ 且未知.

输出: 1 或者 0.

当 $T=e(g_0,h_0)^{a^nf(a)br}$ 时输出 1, 或者 $T\neq e(g_0,h_0)^{a^nf(a)br}$ 时输出 0, 称成功解决 (m,n,f)-GDDHE 问题. 令 (m,n,f)-GDDHE 问题的一个实例为 $\mathcal{I}$, 定义多项式算法 $\mathcal{D}$ 成功解决 (m,n,f)-GDDHE 问题的优势为:

$$Adv^{(m,n,f)\text{-GDDHE}}(\lambda)=\left|\Pr\left[\mathcal{D}\left(\mathcal{I},T=e(g_0,h_0)^{a^nf(a)br}\right)=1\right]-\Pr\left[\mathcal{D}\left(\mathcal{I},T\neq e(g_0,h_0)^{a^nf(a)br}\right)=1\right]\right|.$$

定理 1. 在广义群模型中, (m,n,f)-GDDHE 问题是困难的.

证明: 在困难性分析中考虑最简单的情况, 即 $\mathbb{G}_1=\mathbb{G}_2$. 设 $h_0=g_0^{\eta}$, 则 (m,n,f)-GDDHE 问题可化简为:

$$P=\begin{pmatrix} 1, a, ar, f(a)^2br, & & & & \\ f(a)b, & f(a)ab, & f(a)a^2b, & \ldots, & f(a)a^mb, \\ \eta, & \eta a, & \eta a^2, & \ldots, & \eta a^m, \\ \eta f(a)b, & \eta f(a)ab, & \eta f(a)a^2b, & \ldots, & \eta f(a)a^{n-2}b, \\ \eta f(a)^2b, & \eta f(a)^2ab, & \eta f(a)^2a^2b, & \ldots, & \eta f(a)^2a^mb, \end{pmatrix},\quad Q=1,\quad F=\eta a^nf(a)br.$$

根据文献 [35], 需证明 F 与 (P,Q) 无关, 即不存在系数 $x_{i,j}$ 和 y_1 使得

$$\eta a^nf(a)br=F=\sum x_{i,j}d_id_j+y_1,$$

其中, $d_i,d_j\in P$. 为满足上述等式, 任意两个 P 中元素的乘积必须包含 $\eta f(a)br$. 在下式 P' 中列出所有可能的乘积, 并需证明不存在 P' 中的线性组合满足 F:

$$P'=\left(\eta f(a)b\cdot ar,\eta f(a)ab\cdot ar,\eta f(a)a^2b\cdot ar,\ldots,\eta f(a)a^{n-2}b\cdot ar\right).$$

P' 中任何一个与 $\eta f(a)br$ 有关的线性组合都可写出如下形式:

$$\eta a^nf(a)br=A(a)\eta f(a)br \tag{1}$$

其中, $A(a)$ 的一个多项式, $1 \leqslant degA(a) \leqslant n-1$. 公式 (1) 进一步化简得到:

$$a^n - A(a) = 0 \tag{2}$$

又 $degA(a) \leqslant n-1$, 则 $a^n - A(a)$ 是一个阶为 n 的多项式, 其中 a^n 的系数为 1, $degA(a)$ 表示以 a 为变量的多项式 A 的最高次数. 对任意的多项式 $A(x)$, 多项式 $a^n - A(a)$ 不可能恒等于 0, 与 a 无关. 因此, 不存在系数 $x_{i,j}$ 和 y_1 使得 $F = \sum x_{i,j} d_i d_j + y_1$, 即本文定义的 (m,n,f)-GDDHE 问题是一个难解的 GDDHE 问题. 证毕.

3 标识撤销加密

本节给出撤销加密在标识系统中的形式化定义和相应的安全模型. 为描述方便, 仅给出密钥封装的形式化定义, 即加密算法的输出为封装密钥.

3.1 形式化定义

一个标识撤销加密方案 $\prod$=(Setup, KeyGen, Encrypt, Decrypt), 是由以下 4 个算法组成.

- 系统建立算法 Setup(λ, m): 该算法输入安全参数 λ 和最大撤销用户数量 m, 输出系统主公/私钥对 (mpk, msk).
- 密钥生成算法 KeyGen(mpk, msk, ID): 该算法输入主公/私钥对 (mpk, msk) 和用户标识 ID, 输出密钥 sk_{ID}.
- 加密算法 Encrypt(mpk, R): 该算法输入主公钥 mpk 和一个需要撤销的用户集合 R, 输出密钥 K 和密文 CT.
- 解密算法 Decrypt$(mpk, CT, R, ID, sk_{ID})$: 该算法输入主公钥 mpk, 密文 CT, 撤销用户标识集合 R, 解密者标识 ID 及其密钥 sk_{ID}, 若 $ID \notin R$, 输出密钥 K.

标识撤销加密方案 $\prod$ 需要满足如下正确性: 对任意的撤销集合 R, 以及 $(mpk, msk) \leftarrow$ Setup(λ, m), $sk_{ID} \leftarrow$ KeyGen(mpk, msk, ID) 和 $(K, CT) \leftarrow$ Encrypt(mpk, R), 以下等式成立:

$$\begin{cases} \text{Decrypt}(mpk, CT, R, ID, sk_{ID}) = K, & \text{if } ID \notin R \\ \text{Decrypt}(mpk, CT, R, ID, sk_{ID}) = \perp, & \text{if } ID \in R \end{cases}.$$

3.2 安全性定义

令 $\prod$ 是一个标识撤销加密方案, 对任意多项式时间内的攻击者 $\mathcal{A}$ 和挑战者 C, 选择性 CPA 不可区分安全模型 (IND-sID-CPA) 通过以下游戏定义. 在该定义中, 假设 $\mathcal{A}$ 和 C 都已知撤销用户的最大数量 m.

初始化阶段: $\mathcal{A}$ 输出挑战标识集合 $R^* = (ID_1^*, ID_2^*, \ldots, ID_n^*)$, 其中 $n \leqslant m$, 并将 R^* 发送给 C.

系统建立阶段: C 生成系统主公/私钥对 $(mpk, msk) \leftarrow$ Setup(λ, m), 并将 mpk 发送给 $\mathcal{A}$.

询问阶段 1: $\mathcal{A}$ 将 $ID_i \in R^*$ 发送给 C 询问密钥, C 返回 KeyGen(mpk, msk, ID_i). 此过程允许 $\mathcal{A}$ 根据需要发起多次询问.

挑战阶段: C 生成挑战密钥和密文 $(K^*, CT^*) \leftarrow$ Encrypt(mpk, R^*), 选择一个随机比特 $c \in \{0,1\}$, 设 $K_c = K^*$, 发送 (CT^*, K_0, K_1) 给 $\mathcal{A}$, 其中 K_{1-c} 为 C 选的随机密钥.

询问阶段 2: $\mathcal{A}$ 继续询问 $ID_i \in R^*$ 的密钥, C 返回 KeyGen(mpk, msk, ID_i), 此过程允许 $\mathcal{A}$ 根据需要发起多次询问.

猜测阶段: $\mathcal{A}$ 输出猜测比特 $c' \in \{0,1\}$. 如果 $c' = c$, 则 $\mathcal{A}$ 获胜.

在上述游戏中, $\mathcal{A}$ 的优势定义为:

$$Adv_{\mathcal{A}}^{\text{IND-sID-CPA}}(\lambda) = \left| \Pr[c' = c] - \frac{1}{2} \right|.$$

定义 1 (ND-sID-CPA 安全性). 在 IND-sID-CPA 安全模型中, 若对任意敌手 $\mathcal{A}$, $Adv_{\mathcal{A}}^{\text{IND-sID-CPA}}(\lambda)$ 都是可忽略的, 则称方案 $\prod$ 是 IND-sID-CPA 安全的.

4 SM9 撤销加密方案

本节给出基于 SM9 的用户撤销加密方案的具体构造, 并在定义的复杂性假设中分析方案的安全性. 基于 (m,n,f)-GDDHE 假设, 证明方案满足 IND-sID-CPA 的安全性.

4.1 算法描述

● Setup. 令安全参数为 λ, 撤销允许的最大用户数量为 m, 密钥生成中心首先基于安全参数生成一个非对称双线群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$, 其中 p 为大素数且 $p>2^{\lambda}$, 并随机选择群 $\mathbb{G}_1,\mathbb{G}_2$ 的生成元 g,h. 选择随机数 $\alpha,\beta,\gamma\in\mathbb{Z}_p^*$, 密码函数 $H:\{0,1\}^*\to\mathbb{Z}_p^*$, 密钥派生函数 $KDF:(\mathbb{G}_1)^2\times\mathbb{G}_T\times\left(\mathbb{Z}_p^*\right)^2\to\{0,1\}^{\ell}$, 其中 ℓ 为封装密钥的长度. 计算 $v=e(g,h)^{\alpha\beta}$, 输出如下系统主公私钥对, 其中 hid 为一个字节大小的识别符.

$$mpk=\left(\mathcal{BP},g,h,g^{\alpha},\left\{g^{\gamma\alpha^i}\right\}_{i=0}^{m},\left\{h^{\gamma\alpha^i}\right\}_{i=0}^{m},v,H,KDF,hid,\ell\right),\ msk=(\alpha,\beta,\gamma).$$

● KeyGen. 已知用户标识 $ID\in\{0,1\}^*$, 计算:

$$sk_{ID}=(d_1,d_2)=\left(h^{\frac{\alpha}{H(ID\|hid,p)+\alpha}},h^{\beta+\frac{\gamma}{H(ID\|hid,p)+\alpha}}\right)$$

作为用户的解密密钥, 并通过安全信道发送 sk_{ID} 给用户.

● Encrypt. 已知撤销用户集合 $R=(ID_1,ID_2,\ldots,ID_n)(n\leqslant m)$, 加密者选取随机数 $k\in\mathbb{Z}_p^*$, 计算:

$$w=v^k,\quad C_1=(g^{\alpha})^k,\quad C_2=g^{k\cdot\gamma\cdot\prod_{i=1}^{n}(\alpha+H(ID_i\|hid,p))},\quad \tau=\prod_{ID_i\in R}H(ID_i\|hid,p)\ \bmod\ p,\quad K=KDF(C_1,C_2,w,\tau,\ell),$$

并输出 (C_1,C_2,K), 其中 $CT=(C_1,C_2)$ 为封装密文, K 为封装密钥.

● Decrypt. 设待解密的封装密文为 $CT=(C_1,C_2)$, 对应撤销用户集合为 R, 解密者 $ID\notin R$ 首先根据撤销用户集合 R 定义多项式:

$$f(x)=\prod_{ID_i\in R}(x+H(ID_i\|hid,p))\ \bmod\ p,$$

则

$$\begin{aligned}\frac{f(x)}{x+H(ID\|hid,p)}&=\frac{(x+H(ID_1\|hid,p))(x+H(ID_2\|hid,p))\ldots(x+H(ID_n\|hid,p))}{x+H(ID\|hid,p)}\\&=t_{n-1}x^{n-1}+t_{n-2}x^{n-2}+\ldots+t_1x+t_0+\frac{z}{x+H(ID\|hid,p)}\ \bmod\ p,\end{aligned}$$

其中, $\{t_i\}_{i\in[0,n-1]}$ 是模 p 的系数, 且 $z=f(-H(ID\|hid,p))\neq 0$. 接着利用密钥 sk_{ID} 计算:

$$w'=e(C_1,d_2)\cdot\left(\frac{e(C_2,d_1)}{e\left(C_1,\prod_{i=0}^{n-1}h^{\gamma t_i\alpha^i}\right)}\right)^{-\frac{1}{z}}.$$

最后, 解密者计算:

$$\tau'=\prod_{ID_i\in R}H(ID_i\|hid,p),\ \ K'=KDF(C_1,C_2,w',\tau',\ell).$$

4.2 正确性分析

假设密文 $CT=(C_1,C_2)$ 对应撤销用户的标识集合为 R, 标识 $ID\notin R$ 且对应的密钥为 sk_{ID}. 系统主公钥 mpk 确定后, hid 和 p 的值是固定的. 为描述方便, 下文使用 $H(ID)$ 代替 $H(ID\|hid,p)$, 则以下公式成立:

$$e(C_1,d_2)=e\left(g^{\alpha k},h^{\beta+\frac{\gamma}{H(ID)+\alpha}}\right)=v^k\cdot e(g,h)^{\frac{\alpha\gamma k}{H(ID)+\alpha}},$$

$$\begin{aligned}\left(\frac{e(C_2,d_1)}{e\left(C_1,\prod_{i=0}^{n-1}h^{t_i\gamma\alpha^i}\right)}\right)^{-\frac{1}{z}}&=\left(\frac{e\left(g^{k\cdot\gamma\cdot\prod_{i=1}^{n}(\alpha+H(ID_i))},h^{\frac{\alpha}{H(ID)+\alpha}}\right)}{e\left(g^{\alpha k},h^{\sum_{i=0}^{n-1}t_i\gamma\alpha^i}\right)}\right)^{-\frac{1}{z}}\\&=\left(\frac{e(g,h)^{\frac{\alpha\gamma kf(\alpha)}{H(ID)+\alpha}}}{e(g,h)^{\alpha k\sum_{i=0}^{n-1}t_i\gamma\alpha^i}}\right)^{-\frac{1}{z}}=\left(\frac{e(g,h)^{\alpha\gamma k\cdot\left(\sum_{i=0}^{n-1}t_i\alpha^i+\frac{z}{H(ID)+\alpha}\right)}}{e(g,h)^{\alpha\gamma k\sum_{i=0}^{n-1}t_i\alpha^i}}\right)^{-\frac{1}{z}}\\&=e(g,h)^{-\frac{\alpha\gamma k}{H(ID)+\alpha}},\end{aligned}$$

$$w' = e(C_1, d_2)\cdot\left(\frac{e(C_2, d_1)}{e\left(C_1, \prod_{i=0}^{n-1} h^{t_i\alpha^i}\right)}\right)^{-\frac{1}{z}}$$
$$= v^k \cdot e(g,h)^{\frac{\alpha\gamma k}{H(ID)+\alpha}} \cdot e(g,h)^{-\frac{\alpha\gamma k}{H(ID)+\alpha}} = v^k = w.$$

因此, 若 $CT = (C_1, C_2)$ 为正确的密文, 且对应的撤销用户集合为 R, 则 $w' = w$, 并有:

$$K' = KDF(C_1, C_2, w', \tau', \ell) = KDF(C_1, C_2, w, \tau, \ell) = K.$$

非撤销用户可以恢复出正确的密钥, 方案满足撤销系统的正确性要求. 当 $ID \in R$ 时, 解密过程中的 $e(g,h)^{\frac{\alpha\gamma k}{H(ID)+\alpha}}$ 无法消去, 进而导致解密不成功.

4.3 安全性分析

定理 2. 若 (m,n,f)-GDDHE 困难假设成立, 基于 SM9 的用户撤销方案在随机谕言机模型下是 IND-sID-CPA 安全的.

证明: 在方案的安全性证明中, 假设敌手 $\mathcal{A}$ 有优势 ϵ 攻破上述撤销加密方案, 且 ϵ 不可忽略, 那么存在模拟者 $\mathcal{B}$ 通过与 $\mathcal{A}$ 交互后, 以不可忽略的优势给出 (m,n,f)-GDDHE 问题的解. $\mathcal{B}$ 以下述 (m,n,f)-GDDHE 问题实例和群 $\mathbb{G}_T$ 中的元素 T 为输入.

$$\begin{cases} g_0, g_0^a, g_0^{ar}, g_0^{f(a)^2br}, \\ g_0^{f(a)b}, g_0^{f(a)ba}, g_0^{f(a)ba^2}, \ldots, g_0^{f(a)ba^m}, \\ h_0, h_0^a, h_0^{a^2}, \ldots, h_0^{a^m}, \\ h_0^{f(a)b}, h_0^{f(a)ba}, h_0^{f(a)ba^2}, \ldots, h_0^{f(a)ba^{n-2}}, \\ h_0^{f(a)^2b}, h_0^{f(a)^2ba}, h_0^{f(a)^2ba^2}, \ldots. h_0^{f(a)^2ba^m}, \end{cases}$$

$\mathcal{B}$ 从 $\mathbb{Z}_p^*$ 中选取 n 个两两不同的随机数 $x_1^*, x_2^*, \ldots, x_n^*$, 并定义:

$$\begin{cases} f(z) = (z+x_1^*)(z+x_2^*)\ldots(z+x_n^*) = \sum_{i=0}^{n} w_i z^i \mod p, \\ f_i(z) = \dfrac{f(z)}{z+x_i^*} = \sum_{j=1}^{n-1} t_j z^j \mod p. \end{cases}$$

初始化阶段: $\mathcal{A}$ 输出挑战的撤销用户集合 $R^* = (ID_1^*, ID_2^*, \ldots, ID_n^*)$, 其中 $n \leqslant m$, 并发送 R^* 给 $\mathcal{A}$.

系统建立阶段: 为生成系统主公钥, $\mathcal{B}$ 首先随机选取 $x, y \in \mathbb{Z}_p^*$, 接着, 在不知道 a,b 的情况下隐式地设 $\alpha = a$, 设 $\beta = x - ya^{n-1}b$, $\gamma = yf(a)b$, 并通过已知问题实例计算以下参数:

$$\begin{cases} g = g_0; \\ h = h_0^{f(a)} = h_0^{\sum_{i=1}^{n} w_i a^i} = \prod_{i=1}^{n} \left(h_0^{a^i}\right)^{w_i}; \\ g^\alpha = g_0^a; \\ g^{\gamma\alpha^i} = \left(g_0^{f(a)ba^i}\right)^y, \ i = 0,1,\ldots,m; \\ h^{\gamma\alpha^i} = \left(h_0^{f(a)^2ba^i}\right)^y, \ i = 0,1,\ldots,m; \\ v = e(g,h)^{\alpha\beta} = e(g_0,h_0)^{af(a)(x-ya^{n-1}b)}. \end{cases}$$

选择密钥派生函数 $KDF: (\mathbb{G}_1)^2 \times \mathbb{G}_T \times \left(\mathbb{Z}_p^*\right)^2 \to \{0,1\}^\ell$, 设系统主公钥为:

$$mpk = \left(\mathcal{BP}, g, h, g^\alpha, \left\{g^{\gamma\alpha^i}\right\}_{i=0}^m, \left\{h^{\gamma\alpha^i}\right\}_{i=0}^m, v, KDF\right).$$

可以看出, mpk 可以通过给定的问题实例计算得到.

哈希询问阶段: $\mathcal{A}$ 可以自适应性地询问标识 ID_i 的哈希值. $\mathcal{B}$ 首先建立初值为空的哈希表 $\mathcal{L}_H = (ID_i, h_i)$, 用于记录哈希的询问和哈希值. 若 ID_i 出现在列表 $\mathcal{L}_H$ 中, $\mathcal{B}$ 返回对应的哈希值 h_i. 否则, 根据以下步骤回复 $\mathcal{A}$.

● 若 $ID_i \notin R^*$, $\mathcal{B}$ 随机选取 $x_i \in \mathbb{Z}_p^*$, 其中 x_i 不属于集合 $(x_1^*, x_2^*, \ldots, x_n^*)$, 若 x_i 等于集合中的某个值, 则重新选取. 设 $h_i = H(ID_i) = x_i$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中.

● 若 $ID_i \in R^*$, $\mathcal{B}$ 设 $h_i = H(ID_i) = x_i^*$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中.

询问阶段 1: 针对标识 $ID_i \in R^*$ 的密钥询问, $\mathcal{B}$ 首先建立初值为空的列表 $\mathcal{L}_K = (ID_i, sk_{ID_i})$ 用于记录询问的标识和返回的密钥. 若 ID_i 已经在列表 $\mathcal{L}_K$ 中, $\mathcal{B}$ 返回对应的密钥 sk_{ID_i}. 否则, $\mathcal{B}$ 获取 ID_i 在列表 $\mathcal{L}_H$ 中对应的元素为 (ID_i, h_i) (若不存在, $\mathcal{B}$ 以 ID_i 为输入, 发起哈希询问并获取 h_i 的值), 计算:

$$d_1 = \prod_{i=0}^{n-1}\left(h_0^{a^{i+1}}\right)^{t_i} = h_0^{f_t(a)a} = h_0^{\frac{af(a)}{a+x_t^2}} = h^{\frac{\alpha}{\alpha+H(ID_t)}}, \qquad d_2 = h_0^{f(a)x}\cdot\prod_{i=0}^{n-2}\left(h_0^{f(a)t_i a^i b}\right)^y = h_0^{f(a)\left(\left(x-ya^{n-1}b\right)+\frac{\gamma f(a)b}{x_t^2+a}\right)} = h^{\beta+\frac{\gamma}{H(ID_t)+\alpha}}.$$

设 $sk_{ID_i} = (d_1, d_2)$, 将 (ID_i, sk_{ID_i}) 添加到列表 $\mathcal{L}_K$ 中, 发送 sk_{ID_i} 给 $\mathcal{A}$. 因此, 当 $ID_i \in R^*$ 时, $\mathcal{B}$ 能正确模拟用户密钥.

挑战阶段: $\mathcal{A}$ 决定询问阶段 1 结束后, $\mathcal{B}$ 计算下式:

$$C_1^* = g_0^{ar}, \quad C_2^* = \left(g_0^{f(a)^2 br}\right)^y, \quad w^* = e\left(g_0^{ar}, h_0^{f(a)}\right)^x \cdot T^{-y}, \quad \tau^* = \prod_{ID_i \in R^*} H(ID_i) \mod p, \quad K^* = KDF(C_1^*, C_2^*, w^*, \tau^*, \ell).$$

随机选择比特 $c \in \{0,1\}$, 设 $K_c = K^*$. 从密钥空间中随机选取一个值设为 K_{1-c}, 并发送挑战密文 (C_1^*, C_2^*, K_0, K_1) 给 $\mathcal{A}$.

令 $k^* = r$, 下列等式成立:

$$C_1^* = g_0^{ar} = (g^\alpha)^{k^*}, \quad C_2^* = \left(g_0^{f(a)^2 br}\right)^y = g^{\gamma f(a)^2 br} = g^{\gamma f(a) k^*} = g^{k^*\cdot\gamma\cdot\prod_{ID_i\in R^*}(H(ID_i)+\alpha)}.$$

若 $T = e(g_0, h_0)^{a^n f(a) br}$, 则有:

$$\begin{aligned} w^* &= e\left(g_0^{ar}, h_0^{f(a)}\right)^x \cdot T^{-y} \\ &= e\left(g_0^{ar}, h_0^{f(a)}\right)^x \cdot e(g_0, h_0)^{-ya^n f(a) br} \\ &= e(g_0, h_0)^{af(a)k^*(x-ya^{n-1}b)} \\ &= e(g, h)^{\alpha\cdot\beta\cdot k^*} \\ &= v^{k^*}. \end{aligned}$$

因此, 当 $T = e(g_0, h_0)^{a^n f(a) br}$ 时, (C_1^*, C_2^*) 是通过加密算法生成的正确密文.

询问阶段 2: $\mathcal{A}$ 继续发起 $ID_i \in R^*$ 的密钥询问, $\mathcal{B}$ 根据询问阶段 1 回复 $\mathcal{A}$.

猜测阶段: $\mathcal{A}$ 输出 $c' \in \{0,1\}$. 若 $c' = c$, $\mathcal{B}$ 输出 1 作为给定困难问题实例的解, 表示 $T = e(g_0, h_0)^{a^n f(a) br}$. 否则输出 0 表示 T 是群 $\mathbb{G}_T$ 中不等于 $e(g_0, h_0)^{a^n f(a) br}$ 的随机元素.

从证明的设置可以看出, 模拟和真实攻击是不可区分的. 接下来, 分析 $\mathcal{B}$ 解决困难问题的概率. 若 $T = e(g_0, h_0)^{a^n f(a) br}$, 根据假设有:

$$\Pr\left[c' = c \mid T = e(g_0, h_0)^{a^n f(a) br}\right] = Adv_{\mathcal{A}}^{\text{IND-sID-CPA}}(\lambda) + \frac{1}{2} = \epsilon + \frac{1}{2}.$$

若 T 是群 $\mathbb{G}_T$ 中不等于 $e(g_0, h_0)^{a^n f(a) br}$ 的随机元素, 我们有 $e\left(g_0^{ar}, h_0^{f(a)}\right)^x \cdot T^{-y}$ 是随机的, 即 w^* 随机. 对 $\mathcal{A}$ 而言, w^* 与 C_1^*, C_2^* 独立无关, 有:

$$\Pr\left[c' = c \mid T \neq e(g_0, h_0)^{a^n f(a) br}\right] = \frac{1}{2}.$$

综上, $\mathcal{B}$ 给出 (m, n, f)-GDDHE 困难问题的解的概率为:

$$Adv^{(n,f)\text{-GDDHE}}(\lambda) = \left|\Pr\left[c' = c \mid T = e(g_0, h_0)^{a^n f(a) br}\right] - \Pr\left[c' = c \mid T \neq e(g_0, h_0)^{a^n f(a) br}\right]\right| = \left|\epsilon + \frac{1}{2} - \frac{1}{2}\right| = \epsilon.$$

4.4 方案性能分析

计算复杂度和存储开销是衡量一个密码方案性能的重要指标, 本节将从这两个方面分析方案, 并与现有高效

标识广播加密 (撤销加密) 进行比较. 为比较的公平性, 只考虑密钥封装, 即不考虑会话密钥加密数据的开销和存储. 表 1 给出了比较所用符号的详细说明, 结果如表 2 和表 3 所示.

表 1 符号说明

符号	符号描述
P	双线性映射
$Exp_i\ (i=1,2)$	非对称群 $\mathbb{G}_i$ 中的指数运算(等价于加法群中的标量乘)
Exp	对称群 $\mathbb{G}$ 中的指数运算
E_t	群 $\mathbb{G}_T$ 中的指数运算
N	一次加密运算允许的最大接收者数量(系统总用户数量)
s	一次加密需撤销的用户的数量
$\lvert\mathbb{G}_i\rvert(i=1,2)$	非对称双线性群 $\mathbb{G}_i$ 中元素的大小
$\lvert\mathbb{G}\rvert$	对称双线性群 $\mathbb{G}$ 中元素的大小
ROM	随机谕言机模型

表 2 计算开销比较

方案	加密	解密	撤销/广播
Delerablée[2]	$Exp_1+(N-s+1)Exp_2+E_t$	$2P+(N-s-1)Exp_2+E_t$	广播
Lewko等人[3]	$(3s+1)Exp+E_t$	$3P+2sExp$	撤销
Liu等人[17]	$Exp_1+(N-s+2)Exp_2+E_t$	$4P+(2(N-s)+2)Exp_2+E_t$	广播
Jiang等人[6]	$(s+2)Exp+E_t$	$3P+sExp+E_t$	撤销
Lai等人[7]	$(N-s+1)Exp_1+Exp_2+E_t$	$2P+(N-s-1)Exp_1+E_t$	广播
本方案	$(s+2)Exp_1+E_t$	$3P+sExp_1+E_t$	撤销

表 3 存储开销和安全性比较

方案	公钥	密钥	密文	困难假设	安全性	ROM
Delerablée[2]	$\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_1\rvert+(N+1)\lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	q-Type	sCPA	√
Lewko等人[3]	$\lvert\mathbb{G}_T\rvert+3\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	$(2s+1)\lvert\mathbb{G}\rvert$	q-Type	sCPA	×
Liu等人[17]	$\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_1\rvert+(N+2)\lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	q-Type	sCCA	√
Jiang等人[6]	$\lvert\mathbb{G}_T\rvert+(2N+3)\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert$	q-Type	sCPA	√
Lai等人[7]	$\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_2\rvert+(N+1)\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	q-Type	sCPA	√
本方案	$\lvert\mathbb{G}_T\rvert+(N+2)\lvert\mathbb{G}_2\rvert+(N+3)\lvert\mathbb{G}_1\rvert$	$2\lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	q-Type	sCPA	√

s 表示一次加密需撤销的用户的数量, 则对应接收者的数量为 $(N-s)$, 本文考虑 s 较小的情况, 即 $(N-s)\gg s$. 从表 2 可知, 当 $(N-s)\gg s$ 时, 本文方案的加密开销和解密开销显著低于广播加密方案, 与文献 [3] 和文献 [6] 相当. 根据表 3 可知, 虽然文献 [3] 中的方案具有定长的公钥且方案安全性不依赖于随机谕言机模型, 但其密文大小与撤销用户的数量线性增加, 其他对比方案均是具有定长的密文. 在存储开销和安全性方面, 本文方案与文献 [6] 相当.

5 结 论

本文基于我国商用密码 SM9 标识加密算法提出一个标识撤销加密方案. 方案具有定长的用户密钥和密文, 与撤销用户的数量无关, 并基于随机谕言机模型证明了方案具有 CPA 的安全性. 方案在计算和存储方面的复杂度与目前的撤销方案整体相当. 本文方案不仅可以看成是标识广播加密的补充, 同时也为 SM9 标识密码提供了一种撤销机制, 当用户的密钥泄露后, 可采用本文方案撤销用户密钥对后续广播的解密权限, 进一步丰富和完善了我国商用密码.

References:

[1] Fiat A, Naor M. Broadcast encryption. In: Proc. of the 13th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 1994. 480–491. [doi: 10.1007/3-540-48329-2_40]

[2] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Proc. of the 13th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Kuching: Springer, 2007. 200–215. [doi: 10.1007/978-3-540-76900-2_12]

[3] Lewko A, Sahai A, Waters B. Revocation systems with very small private keys. In: Proc. of the 2010 IEEE Symp. on Security and Privacy. Oakland: IEEE, 2010. 273–285. [doi: 10.1109/SP.2010.23]

[4] Attrapadung N, Herranz J, Laguillaumie F, Libert B, de Panafieu E, Ràfols C. Attribute-based encryption schemes with constant-size ciphertexts. Theoretical Computer Science, 2012, 422: 15–38. [doi: 10.1016/j.tcs.2011.12.004]

[5] Chen J, Libert B, Ramanna SC. Non-zero inner product encryption with short ciphertexts and private keys. In: Proc. of the 10th Int'l Conf. on Security and Cryptography for Networks. Amalfi: Springer, 2016. 23–41. [doi: 10.1007/978-3-319-44618-9_2]

[6] Jiang P, Lai JC, Guo FC, Susilo W, Au MH, Yang GM, Mu Y, Chen RM. Identity-based revocation system: Enhanced security model and scalable bounded ibrs construction with short parameters. Information Sciences, 2019, 472: 35–52. [doi: 10.1016/j.ins.2018.09.020]

[7] Lai JC, Huang XY, He DB. An efficient identity-based broadcast encryption scheme based on SM9. Chinese Journal of Computers, 2021, 44(5): 897–907 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.00897]

[8] Lai JC, Huang XY, He DB, Ning JT. CCA secure broadcast encryption based on SM9. Ruan Jian Xue Bao/Journal of Software, 2023, 34(7): 3354–3364 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6531.htm [doi: 10.13328/j.cnki.jos.006531]

[9] Tang F, Ling GW, Shan JY. Additive homomorphic encryption schemes based on SM2 and SM9. Journal of Cryptologic Research, 2022, 9(3): 535–549 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000532]

[10] Zhang C, Peng CG, Ding HF, Xu DQ. Searchable encryption scheme based on China state cryptography standard SM9. Computer Engineering, 2022, 48(7): 159–167 (in Chinese with English abstract). [doi: 10.19678/j.issn.1000-3428.0062771]

[11] Zhang XF, Peng H. Blind signature scheme based on SM9 algorithm. Netinfo Security, 2019, 19(8): 61–67 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2019.08.009]

[12] Pu L, Lin C, Wu W, He DB. A public-key encryption with keyword search scheme from SM9. Journal of Cyber Security, 2023, 8(1): 108–118 (in Chinese with English abstract). [doi: 10.19363/J.cnki.cn10-1380/tn.2023.01.08]

[13] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Proc. of the 25th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2005. 258–275. [doi: 10.1007/11535218_16]

[14] Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts). In: Proc. of the 28th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Cologne: Springer, 2009. 171–188. [doi: 10.1007/978-3-642-01001-9_10]

[15] Sakai R, Furukawa J. Identity-based broadcast encryption. IACR Cryptology ePrint Archive, 2007, 2007:217.

[16] Kim J, Susilo W, Au MH, Seberry J. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Trans. on Information Forensics and Security, 2015, 10(3): 679–693. [doi: 10.1109/TIFS.2014.2388156]

[17] Liu X, Liu WR, Wu QH, Liu JW. Chosen ciphertext secure identity-based broadcast encryption. Journal of Cryptologic Research, 2015, 2(1): 66–76 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000061]

[18] Libert B, Paterson KG, Quaglia EA. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In: Proc. of the 15th Int'l Conf. on Practice and Theory in Public Key Cryptography. Darmstadt: Springer, 2012. 206–224. [doi: 10.1007/978-3-642-30057-8_13]

[19] Fazio N, Perera IM. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Proc. of the 15th Int'l Conf. on Practice and Theory in Public Key Cryptography. Darmstadt: Springer, 2012. 225–242. [doi: 10.1007/978-3-642-30057-8_14]

[20] He K, Weng J, Liu JN, Liu JK, Liu W, Deng RH. Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. Xi'an: ACM, 2016. 247–255. [doi: 10.1145/2897845.2897879]

[21] Naor M, Pinkas B. Efficient trace and revoke schemes. In: Proc. of the 4th Int'l Conf. on Financial Cryptography. Anguilla: Springer, 2001. 1–20. [doi: 10.1007/3-540-45472-1_1]

[22] Yoo ES, Jho NS, Cheon JH, Kim MH. Efficient broadcast encryption using multiple interpolation methods. In: Proc. of the 7th Int'l Conf. on Information Security and Cryptology. Seoul: Springer, 2005. 87–103. [doi: 10.1007/11496618_8]

[23] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers. In: Proc. of the 21st Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2001. 41–62. [doi: 10.1007/3-540-44647-8_3]

[24] Halevy D, Shamir A. The LSD broadcast encryption scheme. In: Proc. of the 22nd Annual Int'l Cryptology Conf. Santa Barbara:

Springer, 2002. 47–60. [doi: 10.1007/3-540-45708-9_4]

[25] Goodrich MT, Sun JZ, Tamassia R. Efficient tree-based revocation in groups of low-state devices. In: Proc. of the 24th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2004. 511–527. [doi: 10.1007/978-3-540-28628-8_31]

[26] Delerablée C, Paillier P, Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: Proc. of the 1st Int'l Conf. on Pairing-based Cryptography. Tokyo: Springer, 2007. 39–59. [doi: 10.1007/978-3-540-73489-5_4]

[27] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. Alexandria: ACM, 2008. 417–426. [doi: 10.1145/1455770.1455823]

[28] Li J, Li JW, Chen XF, Jia CF, Lou WJ. Identity-based encryption with outsourced revocation in cloud computing. IEEE Trans. on Computers, 2015, 64(2): 425–437. [doi: 10.1109/TC.2013.208]

[29] Ge AJ, Wei PW. Identity-based broadcast encryption with efficient revocation. In: Proc. of the 22nd IACR Int'l Conf. on Practice and Theory of Public-key Cryptography. Beijing: Springer, 2019. 405–435. [doi: 10.1007/978-3-030-17253-4_14]

[30] Susilo W, Chen RM, Guo FC, Yang GM, Mu Y, Chow YW. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in ibbe without knowledge of the plaintext. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. Xi'an: ACM, 2016. 201–210. [doi: 10.1145/2897845.2897848]

[31] Lai JC, Mu Y, Guo FC, Susilo W, Chen RM. Anonymous identity-based broadcast encryption with revocation for file sharing. In: Proc. of the 21st Australasian Conf. Melbourne: Springer, 2016. 223–239. [doi: 10.1007/978-3-319-40367-0_14]

[32] Cheng ZH. Security analysis of SM9 key agreement and encryption. In: Proc. of the 14th Int'l Conf. on Information Security and Cryptology. Fuzhou: Springer, 2019. 3–25. [doi: 10.1007/978-3-030-14234-6_1]

[33] Wang MD, He WG, Li J, Mei R. Optimal design of R-ate pair in SM9 algorithm. Communications Technology, 2020, 53(9): 2241–2244 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-0802.2020.09.025]

[34] Hu XY, He DB, Peng C, Luo M, Huang XY. A fast implementation of R-ate pairing in SM9 algorithm. Journal of Cryptologic Research, 2022, 9(5): 936–948 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000559]

[35] Boneh D, Boyen X, Goh EJ. Hierarchical identity based encryption with constant size ciphertext. In: Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Aarhus: Springer, 2005. 440–456. [doi: 10.1007/11426639_26]

附中文参考文献:

[7] 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. [doi: 10.11897/SP.J.1016.2021.00897]

[8] 赖建昌, 黄欣沂, 何德彪, 宁建廷. 基于 SM9 的 CCA 安全广播加密方案. 软件学报, 2023, 34(7): 3354–3364. http://www.jos.org.cn/1000-9825/6531.htm [doi: 10.13328/j.cnki.jos.006531]

[9] 唐飞, 凌国玮, 单进勇. 基于国密 SM2 和 SM9 的加法同态加密方案. 密码学报, 2022, 9(3): 535–549. [doi: 10.13868/j.cnki.jcr.000532]

[10] 张超, 彭长根, 丁红发, 许德权. 基于国密 SM9 的可搜索加密方案. 计算机工程, 2022, 48(7): 159–167. [doi: 10.19678/j.issn.1000-3428.0062771]

[11] 张雪锋, 彭华. 一种基于 SM9 算法的盲签名方案研究. 信息网络安全, 2019, 19(8): 61–67. [doi: 10.3969/j.issn.1671-1122.2019.08.009]

[12] 蒲浪, 林超, 伍玮, 何德彪. 基于 SM9 的公钥可搜索加密方案. 信息安全学报, 2023, 8(1): 108–118. [doi: 10.19363/J.cnki.cn10-1380/tn.2023.01.08]

[17] 刘潇, 刘巍然, 伍前红, 刘建伟. 选择密文安全的基于身份的广播加密方案. 密码学报, 2015, 2(1): 66–76. [doi: 10.13868/j.cnki.jcr.000061]

[33] 王明东, 何卫国, 李军, 梅瑞. 国密 SM9 算法 R-ate 对计算的优化设计. 通信技术, 2020, 53(9): 2241–2244. [doi: 10.3969/j.issn.1002-0802.2020.09.025]

[34] 胡芯忆, 何德彪, 彭聪, 罗敏, 黄欣沂. 一种 SM9 算法 R-ate 对的快速实现方法. 密码学报, 2022, 9(5): 936–948. [doi: 10.13868/j.cnki.jcr.000559]

赖建昌(1988－), 男, 博士, 副教授, 主要研究领域为公钥密码学, 信息安全.

黄欣沂(1981－), 男, 博士, 副教授, 博士生导师, CCF 专业会员, 主要研究领域为公钥密码学, 信息安全.

何德彪(1980－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为密码学, 信息安全.

陈立全(1976－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为移动信息安全, 物联网系统与安全, 深度学习.

杨少军(1986－), 男, 博士, 副研究员, 主要研究领域为格理论及其应用.