基于 SM9 的密钥策略属性基加密及快速解密

刘晓红[1] 黄欣沂[2] 程朝辉[3] 伍 玮[4]

[1](福建师范大学计算机与网络空间安全学院 福州 350117)

[2](香港科技大学(广州)信息枢纽人工智能学域 广州 511455)

[3](深圳市奥联信息安全技术有限公司 广东 深圳 518052)

[4](香港科技大学(广州)教育科学学院 广州 511455)

摘 要 属性基加密是一种通过指定访问策略实现数据共享的公钥加密技术,分为密钥策略属性基加密和密文策略属性基加密两种.在属性基加密中,数据拥有者通过指定一个访问策略(属性集合)对数据进行加密,被授权的接收者使用与属性集合(访问策略)相关联的解密密钥访问数据.与传统"一对一"的数据共享模式相比,属性基加密是一种更为精细的数据共享机制,可以提供"一对多"的数据共享模式,适用于区块链、云计算等信息系统中的多用户数据安全共享应用.SM9 标识加密是我国设计的标识密码算法,用于保障数据的机密性,于 2021 年成为国际标准.但是,SM9 标识加密仅提供"一对一"的数据共享模式.本文在 SM9 标识加密的基础上,结合经典密钥策略属性基加密的构造思路,构造了一种基于 SM9 的密钥策略属性基加密方案.所提方案中的密钥/密文结构与 SM9 标识加密算法中的密钥/密文结构相似,可与现有使用 SM9 的信息系统有效融合.在此基础上,提出基于 SM9 的密钥策略属性基加密快速解密方法.新方法具有以下特点:(1)通过增加密钥长度,将解密时使用的双线性运算数量由原来的 $2|I|$ 个降低至 2 个,其中 $|I|$ 表示解密时使用的线性秘密生成矩阵中的行数;(2)使用聚合技术,将密文中的群元素个数由原来的 $(2+|S|)$ 个降低至 3 个,其中 S 表示加密时使用的属性集合;(3)新方法具有动态自适应性,用户可以根据实际需求在密钥长度和解密时间之间进行个性化权衡.这些特性使得所提新方法更适用于计算、带宽和存储资源受限的轻量级设备.最后,性能分析表明,该方案在实际应用中是可行的.

关键词 密钥策略属性基加密;SM9;快速解密;定长密文

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.00971

Key-Policy Attribute-Based Encryption Based on SM9 and Its Fast Decryption

LIU Xiao-Hong[1] HUANG Xin-Yi[2] CHENG Zhao-Hui[3] WU Wei[4]

[1](*College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117)

[2](*Artificial Intelligence Thrust, Information Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou* 511455)

[3](*Olym Information Security Technology Ltd., Shenzhen, Guangdong* 518052)

[4](*College of Education Sciences, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou* 511455)

Abstract Attribute-Based Encryption (ABE) is a public-key encryption technology that shares data by specifying an access policy. Based on the different access policy locations, Attribute-Based Encryption falls into two categories: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, the data owner encrypts data by specifying a set of attributes, and authorized recipients use keys associated with the access policy to access the data. In CP-ABE, the data owner encrypts the data by specifying an access policy, and the authorized receiver uses keys associated with a set of attributes to access the data. Compared to traditional "one to-one"

收稿日期:2023-05-15;在线发布日期:2024-01-19.本课题得到国家自然科学基金项目(62032005,62372108)资助.**刘晓红**,博士,主要研究方向为密码学与信息安全.E-mail: xliu854@connect.hkust-gz.edu.cn.**黄欣沂**(通信作者),博士,副教授,主要研究领域为密码学和人工智能.E-mail: xyhuang81@gmail.com.**程朝辉**,博士,主要研究方向为应用密码学和数据安全.**伍 玮**,博士,讲师,主要研究方向为密码学和信息安全.

data sharing mode, ABE provides more fine-grained "one-to-many" data sharing capability, and is suitable for multi-user data security sharing applications in new information systems such as cloud computing, blockchain, and the Internet of Things. SM9 Identity-Based Encryption is one of the series of domestically designed Identity-Based Cryptographic algorithms used to ensure data confidentiality. It has become an international standard in 2021. However, SM9 Identity-Based Encryption only provides "one-to-one" data sharing mode. Based on the SM9 Identity-Based Encryption, this article combines the constructive ideas of the classic KP-ABE, uses Linear Secret Sharing Scheme(LSSS) to represent the access strategy, and proposes a KP-ABE based on SM9. The key/ciphertext structure in the proposed scheme is similar to that in SM9 and can be effectively integrated with existing information systems that use SM9. However, similar to most classic KP-ABE schemes, this scheme suffers from frequent and time-consuming decryption operations. Therefore, based on the aforementioned scheme, a fast decryption method for KP-ABE based on SM9 is proposed. The new method has the following characteristics: (1) the new method reduces the number of pairing operations used in decryption from the original $2|I|$ to 2 by increasing the length of the key, where $|I|$ represents the number of rows in the linear secret sharing matrix used in decryption; (2) the new method uses public key aggregation technology to reduce the number of group elements in the ciphertext from the original $(2+|S|)$ to 3, where S represents the set of attributes used in encryption; (3) the new method has dynamic self-adaptability, and users can make personalized trade-offs between key length and decryption time according to actual needs. For example, in devices with limited storage space, users can shorten the key length by increasing decryption time; In devices with limited computing power, users can reduce decryption time by increasing the length of the key. These features make the proposed new method more suitable for lightweight devices with limited computing, broadband, and storage resources. Finally, security analysis shows that the proposed scheme has the security against Chosen-Plaintext Attack under the $(q,k+1)$- DBDHI assumption, and can achieve the security against Chosen-Ciphertext Attack through FO conversion technology. Performance evaluation shows when the size of the attribute universe is 100 and the number of policy attributes is 50, the decryption time of the fast decryption method is 0.95 s, which is a 69.2% reduction compared to the previous decryption time of 3.09 s.

Keywords key-policy attribute-based encryption; SM9; fast decryption; constant-size ciphertext

1 引 言

随着数字经济的迅速发展,日益增多的数据在互联网中存储、传输、分析和使用.虽然传统的公钥基础设施和标识加密可以提供数据的机密性保护,但仅限于提供"一对一"的数据共享模式.如何在多用户场景中保障数据共享的机密性和灵活性,是相关应用进一步发展面临的关键难题.

属性基加密(Attribute-Based Encryption, ABE)[1]可以为信息系统提供数据机密性保护和细粒度访问控制,是一种将用户和密文分别与策略和属性集合联系起来的公钥加密技术.其中,密钥策略ABE(Key-Policy ABE, KP-ABE)和密文策略 ABE(Ciphertext-Policy ABE, CP- ABE)是 ABE 的两个重要分支.在 KP-ABE 中,访问策略包含在解密密钥中,数据加密者通过属性集合加密数据,解密时,当加密数据对应的属性集合与解密密钥上的访问策略相匹配时,解密成功.CP-ABE 正好相反.

KP-ABE 中"一对多"的访问控制机制使其在处理大量动态变化用户对固定敏感数据的访问控制场景中具有显著优势.例如,在审计日志这一场景中,当需要对日志条目进行加密,但又无法预先确定哪些用户可以访问这些日志条目时,密钥策略属性基加密提供了一个有效的解决方案.通过将日志条目(如用户名称、操作日期和数据类型)表示为一组属

性，加密者可以根据这些属性对数据进行加密. 同时，密钥生成中心会为每一位审计员分发一个与其访问权限相关联的解密密钥，从而精确地控制他们能够访问哪些日志条目. 此外，在付费电视（目标广播）以及视频点播等场景中，内容提供商可以使用密钥策略属性基加密对电视节目或者视频文件进行加密，确保只有付费用户能够解密和观看. 总之，密钥策略属性基加密这一机制不仅可以增强审计日志、付费电视（目标广播）、视频点播等系统中的数据安全性，而且大大提高了访问控制的灵活性.

但是，KP-ABE 中“一对多”的访问控制机制也导致了频繁的解密操作. 这意味着，与加密等其他操作相比，解密操作的使用频率更高. 此外，大部分 KP-ABE 系统的解密操作都包含了双线性配对运算，而相比于其他运算，双线性配对运算最耗时. 而且，很多 KP-ABE 方案中的解密算法需要对解密过程中使用的每个属性进行一次或两次配对运算，解密时间与解密时使用的属性个数成线性关系，这将严重阻碍密钥策略属性基加密算法的实际应用. 此外，传统的密钥属性基加密系统中的密文长度通常与加密时使用的属性个数成线性关系，当加密时使用的属性较多时，将会降低系统的通信效率. 针对此类问题，目前已有的解决办法主要有两种：一种是通过使用聚合技术，以增加密钥长度为代价，减少解密时使用的双线性配对运算数量[2-10]，另一种是将开销较大的解密操作外包给云服务器[11-18]. 但是，这些工作都是围绕国外密码算法展开的，缺少适用于国产密码算法的相关研究.

我国设计了包括数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法的 SM9 系列标识密码算法（简称 SM9）. 2017 年～2021 年，SM9 系列算法陆续成为国际标准. 目前，SM9 已经在多个领域应用，有效保障了国家网络与信息安全. 但是，SM9 设计的初衷是满足网络与信息系统的共性基础安全需求，即保障数据的机密性和不可伪造性，不满足信息系统中用户对数据的细粒度访问控制需求. 目前，对 SM9 标识加密的研究主要集中在算法的安全性分析[19-20]、功能扩展[21-24]和效率优化[25-26]等方面. 在主要的学术期刊和学术会议上，未见基于 SM9 的密钥策略属性基加密的研究成果公开发表. 因此，设计基于 SM9 的密钥策略属性基加密及其快速解密方法具有重要的理论研究意义和实际应用价值.

1.1　相关工作

（1）SM9 标识加密. 1984 年，Shamir[27] 提出了标识加密（Identity-Based Encryption，IBE）系统，减轻了传统公钥密码体制中证书管理产生的负担. 同年，Koblitz[28] 提出了椭圆曲线的概念. 1985 年，Miller[29] 提出了将椭圆曲线应用到密码算法中的新观点. 2001 年，Boneh 和 Franklin[30] 使用椭圆曲线上的双线性映射提出了第一个实用的标识加密算法. 随后，使用椭圆曲线双线性映射构造标识密码算法引起了国内外学者的关注和研究. 例如，2003 年，Canetti、Halevi 和 Katz[31] 提出了前向安全的标识加密方案. 2004 年，Boneh 和 Boyen[32] 提出了无随机谕言模型下选择安全的标识加密方案. 2005 年，Waters[33] 提出了无随机谕言模型下高效的标识加密方案. 2017 年，Döttling 和 Garg[34] 提出了 Diffie-Hellman 假设下安全的标识加密方案.

我国也于 2008 年设计了基于椭圆曲线的公钥密码系列算法 SM9[35]，其中 SM9 标识加密算法于 2020 年成为国家标准，于 2021 年成为国际标准. 自 SM9 系列密码算法发布以来，许多学者对其进行了安全上的分析、功能上的拓展和效率上的优化. Cheng 在文献[19]中分析了 SM9 系列算法的安全性. 赖建昌等人在文献[20]中对 SM9 数字签名算法和密钥封装算法的安全性进行了分析. 秦宝东等人[21] 提出了基于仲裁的 SM9 标识加密方案. 赖建昌等人[22] 提出了基于 SM9 的广播加密方案. 唐飞等人[23] 提出了基于 SM9 的加法同态加密方案. 蒲浪等人[24] 提出了基于 SM9 的可搜索加密系统. 甘植旺和廖方圆[25] 提出了 SM9 中双线性映射 R-ate 的快速计算方法. 王明东等人[26] 提出了 SM9 中双线性映射 R-ate 计算的优化设计.

（2）属性基加密. 2005 年，Sahai 和 Waters[36] 在标识加密算法的基础上，提出了模糊标识加密概念，即属性基加密的雏形. 2006 年，Goyal 等人[1] 将其进一步丰富和完善，形式化定义了属性基加密中的两个分支：密钥策略属性基加密（KP-ABE）和密文策略属性基加密（CP-ABE），并提出了第一个 KP-ABE 系统. 2007 年，Bethencourt、Sahai 和 Waters[37] 提出了第一个 CP-ABE 系统. 但是，现有大多属性基加密[38-40] 中的解密操作都涉及计算开销较大的双线性配对运算.

为了支持快速解密和固定长度的密文大小，2010 年，Herranz 等人[2] 提出了一个具有固定密文长度的门限属性基加密方案. 2011 年，Attrapadung

等人[3]采用聚合技术提出了一个具有固定密文长度的 KP-ABE 方案. 2013 年，Hohenberger 和 Waters[4]提出了一个新的具有固定密文长度和快速解密的 KP-ABE 方案. 2014 年，Lai 等人[5]基于合数阶群提出了一个具有固定密文长度和快速解密的完全安全的 KP-ABE 方案，2017 年，Agrawal 等人[6]提出了支持大属性域的快速解密的属性基加密方案. Kumar 等人[7]于 2022 年提出了一种用于云环境中安全高效的可搜索 KP-ABE 方案. Riepel 等人[8]于 2022 年提出了具有适应性安全的可快速解密的 KP-ABE 和 CP-ABE 方案. Hafizpour 等人[9]于 2023 年提出了一种用于雾计算中可快速加解密的新型 KP-ABE 方案. Jain 等人[10]于 2023 年提出了具有固定长度密钥和密文的功能加密和属性基加密.

为了支持快速解密，也有学者提出将开销较大的解密操作外包的思想. Green 等人[11]于 2011 年引入了外包属性基加密的概念，并结合云计算模型提出了一个将解密操作外包的属性基加密系统. Parno 等人[12]于 2012 年提出了如何利用具有外包解密的 ABE 方案构造多功能可验证计算方案. Lai 等人[13]于 2013 年引入了可验证外包属性基加密的概念，形式化了外包属性基加密的外包计算结果的可验证性. Zhang 等人[14]于 2016 年提出了一个在外包可验证计算中具有固定密文长度的 KP-ABE 方案. Sun 等人[15]于 2017 年提出了一个具有访问控制功能的云平台下外包数据流动态可验证方法. Ning 等人[16]于 2018 年提出了一个 σ 次外包可审计的 CP-ABE 方案. Yang 等人[17]于 2020 年提出了一个轻量级的具有固定密文长度的属性基加密方案. Astudillo[18]于 2023 年研究了支持数据外包的多用户可搜索 KP-ABE.

虽然属性基加密已经取得了丰硕的研究成果，但几乎所有的算法都是由国外标识加密算法衍生的. 为了研究基于国产商用密码 SM9 的属性基加密，Yang 等人[41]于 2019 年提出了一个基于 SM9 的 CP-ABE 方案. Ji 等人[42]也于 2021 年提出了一个基于 SM9 可用于调度和控制云的 CP-ABE 方案. 然而，在主要的学术期刊和学术会议上，未见基于 SM9 的 KP-ABE 及其快速解密方法公开发表.

1.2 技术路线

本文主要采用线性秘密共享方案(Linear Secret Sharing Scheme，LSSS)构造基于 SM9 的 KP-ABE 方案. 具体而言，本文首先在 SM9 标识加密的基础上引入属性空间 $\mathcal{U}$，以及相应的属性公钥 $h_i(i\in[1,\mathcal{U}])$. 其次，在加密阶段，引入属性集合 $S\subseteq\mathcal{U}$. 在 SM9 标识加密的密文结构基础上，增加属性集合 S 所对应的部分密文 $\{C_x\}_{x\in S}$，从而产生与属性集合 S 相关联的密文. 最后，在密钥生成阶段，通过线性秘密共享方案产生系统主密钥 a 针对所有属性的秘密份额 $\lambda_i,i\in[1,l]$，其中 l 是线性秘密生成矩阵的行数，结合 SM9 标识加密的密钥结构，产生与该属性相对应的部分解密密钥 $D_i,i\in[1,l]$. 进而产生与该访问结构相关联的解密密钥 SK. 因此，本文所构造的基于 SM9 的 KP-ABE 最大化的保留了 SM9 标识加密的密钥和密文结构.

本文主要采用公钥聚合技术实现基于 SM9 的 KP-ABE 的快速解密(如图 1). 在密钥生成阶段，本文对基于 SM9 的 KP-ABE 中的密钥结构进行适当改进，通过在密钥中增加一些“辅助参数”，满足解密时对密钥进行聚合的条件. 在解密阶段，首先使用公钥聚合技术将密文中与属性相关的部分密文 C_i 聚合成一个群元素 L. 其次，使用公钥聚合技术对解密密钥进行聚合，将访问结构矩阵中每一行所对应的部分密钥 $D_{i,j}$ 聚合产生 D_i. 最后，将密文聚合的结果 L 与密钥聚合的结果 D_i 进行双线性配对运算. 从而降低解密操作中使用的配对运算数量，实现快速解密和定长密文.

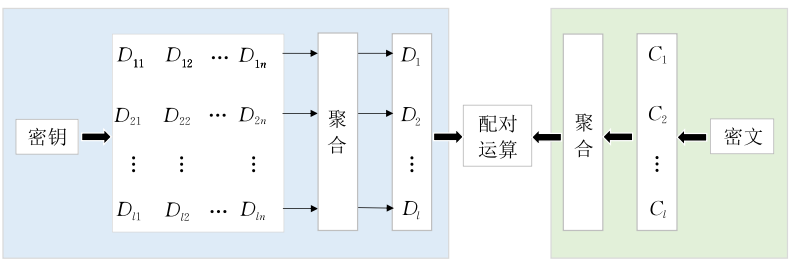


图 1 快速解密方法

1.3 本文贡献

本文借鉴经典密钥策略属性基加密的构造思路，结合国产 SM9 标识密码的结构特点，提出了基于 SM9 的密钥策略属性基加密算法及其快速解密

方法.

(1)本文利用更实用的 LSSS 提出了一种基于 SM9 的密钥策略属性基加密方案.该方案最大程度的保留了 SM9 标识密码算法中的密钥、密文结构,可与现有使用 SM9 的信息系统有效融合.在$(q,k+1)$-DBDHI 假设下,该方案满足选择集合-选择明文攻击安全性,可以通过 FO 转换技术[43]实现选择密文攻击安全性.

(2)本文提出了一种基于 SM9 的密钥策略属性基加密快速解密方法.该方法通过在密文上使用聚合技术,将密文长度由原来的$2+|S|$个群元素降低至 3 个群元素,其中 S 表示加密时使用的属性集合.另外,该方法通过使用聚合技术,将解密时使用的配对运算数量由原来的$2|I|$个降低至了现在的 2 个,其中$|I|$表示解密时使用的线性秘密生成矩阵中的行数.因此,该方法可以实现固定长度的密文和快速解密.

(3)本文所提出的快速解密方法支持动态自适应的解密操作,用户可以结合实际应用需求,在密钥长度和解密时间之间进行个性化权衡.在存储空间受限的设备中,用户可以通过增加解密时间来缩短密钥长度;在计算能力受限的设备中,用户可以通过增加密钥长度来降低解密时间.该权衡不需要改变算法的参数设置、密钥生成和加密操作,仅需要对解密操作进行特定调整即可实现.

(4)本文对所提出的基于 SM9 的 KP-ABE 方案、快速解密方案以及国外经典快速解密方案进行了通信代价和计算代价的比较.另外,在策略属性数量分别为 10、20、30、40、50 时,对所提出的两个方案进行了编程实现,实验结果显示快速解密方案可以将解密时间降低至少 69.2%.

1.4　文章结构

第 2 节回顾与本文相关的基础知识;第 3 节提出基于 SM9 的 KP-ABE 方案,并在$(q,k+1)$-DBDHI 假设下证明方案的安全性;第 4 节提出基于 SM9 的 KP-ABE 快速解密方法;第 5 节对所提出的方案进行性能分析和编程实现;第 6 节对本文的工作进行总结.

2　预备知识

本节介绍双线性群、困难问题假设、线性秘密共享方案、KP-ABE 的形式化定义和安全模型以及 SM9 标识加密算法等基础知识.

2.1　双线性群

设存在一个五元组$BP=(G_1,G_2,G_T,e,N)$,其中 N 是与安全参数 λ 相关的大素数.G_1,G_2 是 N 阶加法群,G_T 是 N 阶乘法群.$e:G_1\times G_2\to G_T$ 满足如下性质:

(1)双线性(Bilinearity).对所有的 $P\in G_1,Q\in G_2$ 和 $a,b\in Z_N^*$,有 $e(aP,bQ)=e(P,Q)^{ab}$ 成立;

(2)非退化性(Non-degeneracy).存在 $P\in G_1,Q\in G_2$,使得 $e(P,Q)\neq 1$.

对所有的 $P\in G_1,Q\in G_2$,存在计算 $e(P,Q)$ 的有效算法.则称 BP 是一个双线性群.

2.2　困难问题

定义 1.　(q,k)-Decisional Bilinear Diffie-Hellman Inverse((q,k)-DBDHI)问题[44].

设$BP=(G_1,G_2,G_T,e,N)$是一个双线性群,$P\in G_1,Q\in G_2$.已知

$$I=\left(c,P,bP,aP,a^2P,\cdots,a^{k+1}P,Q,bQ,aQ,a^2Q,\cdots,a^qQ,\frac{1}{(a+c)^2}Q,\frac{1}{(a+c)^3}Q,\cdots,\frac{1}{(a+c)^k}Q\right)$$

和一个随机的群元素 $T\in G_T$,判断 $T=e(P,Q)^{\frac{b}{a+c}}$ 是否成立.

2.3　访问结构

定义 2.　访问结构[45].设$\{P_1,P_2,\cdots,P_n\}$是一个参与者的集合.对于集合 $\mathbb{A}\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$,如果$\forall B,C\subseteq\{P_1,P_2,\cdots,P_n\},B\in\mathbb{A},B\subseteq C\Rightarrow C\in\mathbb{A}$,则称 $\mathbb{A}$ 是一个(单调)访问结构.

2.4　线性秘密共享方案(LSSS)

定义 3.　线性秘密共享方案(LSSS)[45].假设$\mathcal{U}$表示一个属性空间,p 表示一个素数,$\mathbb{Z}_p$上的秘密共享方案 Π 应满足以下条件:

(1)每个属性对应秘密值$s\in\mathbb{Z}_p$的一个秘密份额.

(2)针对任意的访问策略 $\mathbb{A}$,存在一个对应的矩阵 $\boldsymbol{M}_{l\times n}$和映射 $\rho(i)$.其中 $\boldsymbol{M}_{l\times n}$称为秘密生成矩阵,映射 $\rho(i)$将矩阵 $\boldsymbol{M}$ 中的第 $i(i=1,2,\cdots,l)$行映射到属性空间$\mathcal{U}$中的特定属性 $\rho(i)$上.构造向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)$,其中,$r_2,r_3,\cdots,r_n\in\mathbb{Z}_p$,则 $\lambda_i=(\boldsymbol{M}\cdot\boldsymbol{v})_i,i\in[1,l]$就是属性 $\rho(i)$对应的秘密份额.

如果 S 是一个授权集合,选择 $I=\{i\in[l]\wedge\rho(i)\in S\}$.假设$\{\lambda_i=(\boldsymbol{M}\cdot\boldsymbol{v})_i\}_{i\in I}$是 s 对应的秘密份额,则存在可被计算出来的常数集合$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$,

使得$\sum_{i\in I}\omega_i\cdot\lambda_i=s$. 如果 S'是一个未被授权的集合，则不存在上述所计算的$\{\omega_i\}_{i\in I}$.

2.5 KP-ABE 的形式化定义和安全模型

如图 2 所示，一个 KP-ABE 系统定义如下.

(1) Setup(λ)→(mpk,msk)，系统建立算法. 给定安全参数 λ，该算法输出主公钥 mpk 和主私钥 msk.

(2) Encrypt(mpk,m,γ)→ct，加密算法. 给定 mpk，明文 m 和集合 γ，该算法输出与 γ 相对应的密文 ct.

(3) KeyGen(mpk,msk,$\mathbb{A}$)→$sk_{\mathbb{A}}$，密钥生成算法. 给定 mpk，msk 和访问策略 $\mathbb{A}$，该算法输出与 $\mathbb{A}$ 相关联的解密密钥 $sk_{\mathbb{A}}$.

(4) Decrypt(mpk,$sk_{\mathbb{A}}$,ct)→m 或者$\perp$，解密算法. 给定 mpk，对应于访问策略 $\mathbb{A}$ 的密钥 $sk_{\mathbb{A}}$ 和对应于集合 γ 的密文 ct. 如果 γ 匹配 $\mathbb{A}$，即 $\gamma\in\mathbb{A}$，则该算法输出 m，否则输出$\perp$.

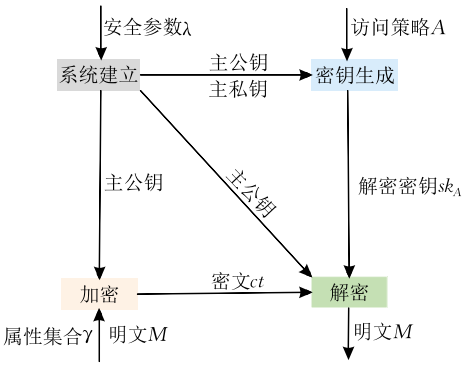


图 2 KP-ABE 的工作流程图

密钥策略属性基加密算法的正确性要求：对于任意的安全参数 λ，任意的(mpk,msk)←Setup(λ)，任意的明文 m，任意的属性集 γ 和访问策略 $\mathbb{A}$，当且仅 $\gamma\in\mathbb{A}$ 时，下面的等式成立：

$$\text{Decrypt}(mpk,\text{Keygen}(mpk,msk,\mathbb{A}),\text{Encrypt}(mpk,m,\gamma))\rightarrow m.$$

文献[1]定义了密钥策略属性基加密系统的选择集合安全模型(Selective-Set Model)，其安全性主要通过一个挑战者 C 和一个攻击者$\mathcal{A}$之间的交互游戏来定义(如图 3)，具体描述如下：

初始化阶段：攻击者$\mathcal{A}$首先声称他想要攻击的属性集 γ；

系统建立阶段：C 运行系统建立算法，生成 mpk 和 msk，并将 mpk 发送给$\mathcal{A}$.

询问阶段 1：$\mathcal{A}$询问与访问策略 $\mathbb{A}_j$ 相关的解密密钥，其中对 $\forall j$ 有 $\gamma\notin\mathbb{A}_j$，C 运行密钥生成算法生成相应解密密钥 $sk_{\mathbb{A}_j}$，并将其发送给$\mathcal{A}$.

挑战阶段：$\mathcal{A}$选择消息 M_0 和 M_1，C 选择 $\beta\in\{0,1\}$，在属性集 γ 下加密 M_β 生成密文 ct^*，并将其发送给$\mathcal{A}$.

询问阶段 2：重复询问阶段 1.

猜测阶段：$\mathcal{A}$输出猜测 β'. 如果 $\beta'=\beta$，则称$\mathcal{A}$获胜，获胜优势为 $Adv_{\mathcal{A}}=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$.

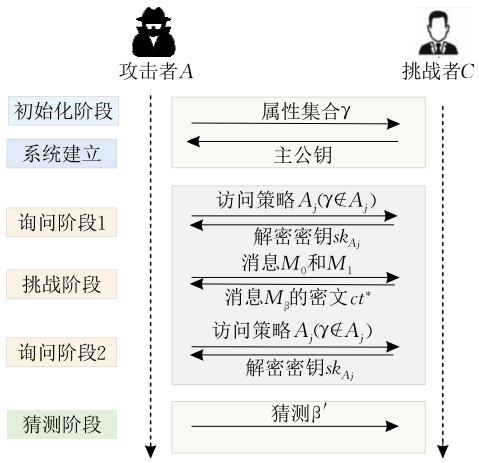


图 3 KP-ABE 的安全模型

定义 4. 在上述游戏中，如果对于任意小的 $\varepsilon\in N^+$，有 $Adv_{\mathcal{A}}\leq\varepsilon$，则称该 KP-ABE 方案在选择集合/明文攻击下是安全的，即 IND-SST-CPA 安全(Indistinguishability against Selective-Set, Chosen Plaintext Attack).

2.6 SM9 标识加密方案

SM9 标识加密方案是基于有限域椭圆曲线群构造的，包括以下四个多项式时间算法[35]：

Setup(λ)：给定安全参数 λ，双线性群 $BP=(G_1,G_2,G_T,e,N)$，哈希函数 $H_1:\{0,1\}^*\rightarrow Z_N^*$，一个字节表示的私钥生成函数标识符 hid，该算法随机选择 $P_1\in G_1$，$P_2\in G_2$ 和随机数 $a\in Z_N$，计算 $P_{pub}=aP_1$ 和设置 $g=e(P_{pub},P_2)$.

公共参数 $mpk=\{BP,P_1,P_2,P_{pub},g,H_1,hid\}$，主私钥 $msk=a$.

KeyGen(mpk,msk,ID)：给定一个标识 ID，该算法首先计算 $t_1=H_1(ID\|hid,N)+a(\text{mod}\,N)$. 如果 $t_1=0$，密钥生成中心 KGC 重新选择主密钥 $a\in Z_N$，计算并公开相应的主公钥 P_{pub} 和 g，重新计算现有用户的解密密钥 sk. 否则，它计算 $t_2=at_1^{-1}$ 和 $sk_{ID}=t_2P_2=\dfrac{a}{H_1(ID\|hid,N)+a}P_2$.

Encrypt(mpk,M,ID)：给定一个标识 ID，该算法首先选择随机数 $s\in\mathbb{Z}_N$，并计算 $Q_{ID}=H_1(ID\|hid,N)P_1+P_{pub}$. 然后，它计算密文 $ct=(C_1=Mg^s, C_2=sQ_{ID})$.

Decrypt(mpk,ct,sk_{ID})：一旦收到一个密文 ct 和一个解密密钥 sk_{ID}，该算法首先计算 $w=e(C_2, sk_{ID})$，然后输出明文消息 $M=C_1/w$.

3　基于 SM9 的 KP-ABE

本节首先提出基于 SM9 的 KP-ABE 方案(也称基础方案)，然后在此基础上，提出基于 SM9 的 KP-ABE 快速解密方法(也称改进方案).

3.1　方案描述

设 G_1,G_2 是阶为 N 的加法群，G_T 是阶为 N 乘法群. $e:G_1\times G_2\to G_T$ 是双线性映射，$H_1:\{0,1\}^*\to Z_p^*$ 是一个抗碰撞的哈希函数. hid 是用一个字节表示的私钥生成函数标识符. 方案中我们用 $H_1(N)$ 来代表 $H_1(N\|hid,N)$. 定义属性空间为 $\mathcal{U}$，且 $|\mathcal{U}|=k$，为简单起见，令 $\mathbb{Z}_N^*$ 中的前 k 个元素作为属性全集，即 $\mathcal{U}=\{1,2,\cdots,k\}$.

Setup(λ)：该算法首先选择生成元 $P_1\in G_1$，$P_2\in G_2$，以及随机数 $a\in Z_N^*$. 然后计算群 G_1 中的元素 $P_{pub}=aP_1$，群 G_T 中的元素 $g=e(P_{pub},P_2)$. 最后从 G_2 中随机选择 k 个互不相同的元素 $h_1,h_2,\cdots,h_k$，分别对应 k 个不同属性.

定义系统的主公钥为

$$mpk=\{P_1,P_2,P_{pub},g,h_1,h_2,\cdots,h_k\},$$

主私钥为 $msk=a$.

Encrypt(mpk,M,γ)：该算法输入主公钥 mpk，要加密的消息 $M\in\mathbb{G}_{T_2}$，属性集 S. 选择随机数 $s\in\mathbb{Z}_N^*$，输出密文 $ct=(S,C,C',C_x)$，其中

$$C=Mg^s, C'=s(H_1(N)P_1+P_{pub}), \{C_x=sh_x\}_{x\in S}.$$

KeyGen(mpk,msk,$\mathbb{A}$)：该算法输入主密钥 msk 和一个 LSSS 结构的访问策略 $(\boldsymbol{W},\rho)$，其中 $\boldsymbol{W}$ 是一个 $l\times n$ 的矩阵，函数 ρ 将 $\boldsymbol{W}$ 中的行映射到属性集中的属性上. 算法首先选择一个随机的向量 $\boldsymbol{v}=(a,y_2,y_3,\cdots,y_n)\in Z_N^n$，这些值将被用来分享主密钥 a. 其次对于 $i=1$ 到 l，该算法计算 $\lambda_i=\boldsymbol{v}\cdot\boldsymbol{W}_i$，其中 $\boldsymbol{W}_i$ 是矩阵 $\boldsymbol{W}$ 中的第 i 行向量. 最后该算法选择随机值 $r_1,r_2,\cdots,r_l\in Z_N$，输出私钥 SK 为

$$D_1=\frac{\lambda_1}{H_1(N)+a}P_2+r_1h_{\rho(1)},\ R_1=r_1(H_1(N)+a)P_1,$$

$$\cdots$$

$$D_l=\frac{\lambda_l}{H_1(N)+a}P_2+r_lh_{\rho(l)},\ R_l=r_l(H_1(N)+a)P_1.$$

Decrypt(mpk,$sk_{\mathcal{A}}$,ct)：该算法输入与访问策略 $(\boldsymbol{W},\rho)$ 相对应的私钥 SK 以及与属性集 S 相对应的密文 ct. 如果 S 不满足访问策略 $(\boldsymbol{W},\rho)$，则算法输出 $\perp$，否则定义 $I\subseteq\{1,2,\cdots,l\}$，且 $I=\{i:\rho(i)\in S\}$. 令 $\{\omega_i\in\mathbb{Z}_N\,|\,i\in I\}$ 为满足如下条件的常数集合：$\sum_{i\in I}\omega_i\boldsymbol{W}_i=(1,0,0,\cdots,0)$(注意 ω_i 的选择不唯一). 该算法计算

$$\frac{\prod_{i\in I}e(C',D_i)^{w_i}}{\prod_{i\in I}e(R_i,C_x)^{w_i}}$$

$$=\frac{\prod_{i\in I}e\left(s(H_1(N)P_1+P_{pub}),\frac{\lambda_i}{H_1(N)+a}P_2+r_ih_{\rho(i)}\right)^{w_i}}{\prod_{i\in I}e(r_i(H_1(N)+a)P_1,sh_x)^{w_i}}$$

$$=\prod_{i\in I}e(sP_1,\lambda_iP_2)^{w_i}$$

$$=e(P_1,P_2)^{\sum_{i\in I}s\lambda_iw_i}$$

$$=e(P_1,P_2)^{sa}$$

$$=g^s.$$

其中 $x=\rho(i)$，最后该算法计算 C/g^s 得到消息 M.

3.2　安全性证明

定理 1.　如果 $(q,k+1)$-DBDHI 假设成立，那么本文提出的方案是 IND-SST-CPA 安全的.

证明.　假设存在 PPT 算法的敌手 A，在 IND-SST-CPA 安全模型下，以不可忽略的优势 ε 攻破上述方案，那么我们可以构造一个模拟者 B 解决 $(q,k+1)$-DBDHI 问题.

B 被给 $(q,k+1)$-DBDHI 问题实例

$$\left(c,P,bP,aP,a^2P,\cdots,a^{k+2}P,Q,bQ,aQ,a^2Q,\cdots,\right.$$

$$\left.a^qQ,\ \frac{1}{(a+c)^2}Q,\ \frac{1}{(a+c)^3}Q,\ \cdots,\ \frac{1}{(a+c)^{k+1}}Q\right)$$

和一个随机的群元素 $T\in G_T$，B 的目标是区分出群 G_T 中的元素 $T=e(P,Q)^{\frac{b}{a+c}}$ 是否成立. 假定属性空间 $\mathcal{U}=\{1,2\cdots,k\}$ 已经确定并且是公开的.

系统建立阶段：模拟者 B 首先从敌手 A 处得到一个挑战的属性集合 S^*，然后按照以下方式构建系统参数：

(1) 从 Z_N^* 中选择不同的随机数 $w_1,w_2,\cdots,w_q$，生成多项式

$$f(x)=\prod_{i=1}^{q}(x+w_i)=\sum_{i=0}^{q}c_i x^i \bmod N;$$

(2) 根据已知问题的实例计算群 G_1 的生成元 $P_1=P$,群 G_2 的生成元 $P_2=f(a)Q$,以及 $P_{pub}=aP_1=aP$ 和 $g=e(P_{pub},P_2)$,注意 a 未知;

(3) 对于 $\forall x\in[1,k]$,选择 Z_N^* 中的随机数 z_x,设置

$$h_x=\begin{cases}z_x(a+c)Q, & x\in S^*;\\ \dfrac{z_x}{(a+c)^{k+2-x}}Q, & x\notin S^*.\end{cases}$$

因为属性 $x\in[1,k]$,所以 $k+2-x\in[2,k+1]$,从而 $\dfrac{1}{(a+c)^{k+2-x}}Q$ 可以通过问题实例计算得到.

最后模拟者 B 输出系统的主公钥 $mpk=(P_1,P_2,P_{pub},g,h_1,h_2,\cdots,h_k)$,主私钥 $msk=a$ 保密,并且设置 $H_1(N)=c$.

私钥询问:A 允许询问访问策略$(\boldsymbol{W},\rho)$的私钥,其中 $\boldsymbol{W}$ 是一个 $l\times n$ 的矩阵,且不能被 S^* 所满足.定义两个集合 $K=\{i|\rho(i)\in S^*\}$ 和 $K'=\{i|\rho(i)\notin S^*\}$,显然有 $K'=[1,l]/K$. 根据如下命题,我们可以找到一个向量 $\boldsymbol{v}$.

命题 1. 一个向量 $\boldsymbol{\pi}$ 与由矩阵 $\boldsymbol{M}$ 表示的一组向量线性无关,当且仅当存在一个向量 $\boldsymbol{v}$ 使得 $\boldsymbol{Mv}=\boldsymbol{0}$ 而 $\boldsymbol{\pi}\cdot\boldsymbol{v}\neq 0$.

因为 S^* 不满足访问策略$(\boldsymbol{W},\rho)$,因此单位向量 $\boldsymbol{e}=(1,0,0,\cdots,0)$不在 $\boldsymbol{W}_i(i\in K)$的张成空间中,由上述命题可知,存在向量 $\boldsymbol{v}$ 使得 $\boldsymbol{W}_i\boldsymbol{v}=0(i\in K)$而 $\boldsymbol{e}\cdot\boldsymbol{v}\neq 0$. 不妨设 $\boldsymbol{v}=(1,v_2,v_3,\cdots,v_n)$,这样的向量可以被有效的计算出来. 现在我们通过向量 $a\boldsymbol{v}$ 进行秘密分享以产生解密密钥,因为 $v_1=1$,所以实际分享的秘密值依然是主密钥 a. 设秘密份额 $\lambda_i=(a\boldsymbol{v})\cdot\boldsymbol{W}_i$.

当 $i\in K$ 时,因为 $\boldsymbol{W}_i\boldsymbol{v}=0$,所以 $\lambda_i=0$,B 设置密钥组件为 $D_i=0\cdot P_2$; $R_i=0\cdot P_1$;

当 $i\notin K$ 时,B 首先计算 $c_i=\boldsymbol{v}\cdot\boldsymbol{W}_i$,然后计算 $\lambda_i=ac_i$ 以及

$$\frac{xf(x)}{x+c}=f'(x)+\frac{E}{x+c},$$

其中 $f'(x)$ 是 q 次多项式,$E\neq 0$ 且可求.

最后 B 选择随机数 $r_i'\in Z_N$,计算密钥组件为

$$D_i=c_i f'(a)Q+r_i' h_x,$$

$$R_i=r_i'(a+c)P-\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)}P.$$

设 $r_i=r_i'-\dfrac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)-1}$,则有

$$\begin{aligned}D_i&=c_i f'(a)Q+r_i' h_x\\&=c_i f'(a)Q+\frac{Ec_i}{a+c}Q+r_i' h_x-\frac{Ec_i}{a+c}Q\\&=c_i f'(a)Q+\frac{Ec_i}{a+c}Q+\Big(r_i+\frac{Ec_i}{z_x}\cdot\\&\quad(a+c)^{k+2-\rho(i)-1}\Big)\frac{z_x}{(a+c)^{k+2-x}}Q-\frac{Ec_i}{a+c}Q\\&=\frac{c_i a f(a)}{a+c}Q+r_i h_{\rho(i)}\\&=\frac{\lambda_i}{a+c}P_2+r_i h_{\rho(i)},\end{aligned}$$

以及

$$\begin{aligned}R_i&=r_i'(a+c)P-\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)}P\\&=\Big(r_i+\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)-1}\Big)(a+c)P-\\&\quad\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)}P\\&=r_i(a+c)P_1.\end{aligned}$$

至此 B 已经构造了一个与访问策略$(\boldsymbol{W},\rho)$相关的有效解密密钥,但是该密钥并不是分布均匀的,所以 B 在将该密钥发送给 A 之前需要对其重新随机化,具体操作如下:

重新随机化:B 选择随机数 $r_i''\in Z_N$,计算

$$D_i'=D_i+r_i'' h_{\rho(i)},$$

$$R_i'=R_i+r_i''(aP+cP)=R_i+r_i''(a+c)P_1.$$

可以看出,通过在每个密钥组件中插入随机数 r_i'',可以使得一个有效的解密密钥变为一个分布良好的解密密钥,与通过密钥生成算法生成的密钥具有相同的分布.

挑战阶段:敌手 A 选择两个等长的消息 M_0 和 M_1,并将其发送给 B. B 随机选择 $v\in\{0,1\}$,并设随机数 $s=\dfrac{b}{a+c}$,则有关于消息 M_v 的密文:

$$C=M_v e(bP,f'(a)Q)T^E;$$

$$C'=bP=\frac{b}{a+c}(a+c)P_1=s(a+c)P_1;$$

$$C_x=z_x bQ=\frac{b}{a+c}z_x(a+c)Q=sh_x.$$

如果 $T=e(P,Q)^{\frac{b}{a+c}}$,则有

$$\begin{aligned}C&=M_v e(bP,f'(a)Q)T^E\\&=M_v e(bP,f'(a)Q)e(P,Q)^{\frac{Eb}{a+c}}\\&=M_v\big[e(P,Q)^{\frac{af(a)}{a+c}}\big]^b=M_v g^s.\end{aligned}$$

因此上述密文是消息 M_v 在属性集合 S^* 下加密的有效密文.

当 $T\neq e(P,Q)^{\frac{b}{a+c}}$ 时，由于 T 是群 G_T 中的随机元素，因此上述密文没有包含 M_v 的任何信息.

询问阶段 2：重复进行密钥询问.

猜测阶段：一旦敌手 A 回复他的猜测 v'，当 $v'=v$ 时，模拟者 B 得到 $T=e(P,Q)^{\frac{b}{a+c}}$，当 $v'\neq v$ 时，模拟器 B 得到 $T\neq e(P,Q)^{\frac{b}{a+c}}$.

最后分析 B 解决 $(q,k+1)$-DBDHI 问题的优势：

(1) 如果 $T=e(P,Q)^{\frac{b}{a+c}}$，那么按照定义，A 至少可以以 ε 的优势攻破上述方案. 也就是说，如果 A 输出 $v'=v$，那么 B 猜测 $T=e(P,Q)^{\frac{b}{a+c}}$ 的概率至少是 $\varepsilon+\frac{1}{2}$.

(2) 否则，A 没有获得任何关于 M_v 的信息. 也就是说，如果 A 输出 $v'\neq v$，那么 B 猜测 $T=e(P,Q)^{\frac{b}{a+c}}$ 的概率是 $\frac{1}{2}$.

综上所述，B 解决 $(q,k+1)$-DBDHI 问题的优势至少是：$\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$.

证毕.

4　基于 SM9 的 KP-ABE 快速解密方法

在第 3 节的基础方案中，解密需要 $2|I|$ 个配对运算，而在程序实现过程中，配对运算是最耗时的，这将严重阻碍方案的运行效率. 本节借鉴文献[4]的构造技术，通过牺牲解密密钥长度来减少解密时使用的双线性配对个数，提出了基于 SM9 的 KP-ABE 快速解密方法，即改进方案，具体如下.

4.1　方案描述

设 G_1，G_2 是阶为 N 的加法群，G_T 是阶为 N 乘法群. $e:G_1\times G_2\rightarrow G_T$ 是双线性映射，$H_1:\{0,1\}^*\rightarrow Z_N^*$ 是用一个字节表示的加密密钥生成函数标识符. 定义属性空间为 $\mathcal{U}$，且 $|\mathcal{U}|=k$，为简单起见，令 $\mathbb{Z}_N^*$ 中的前 k 个元素作为属性全集，即 $\mathcal{U}=\{1,2,\cdots,k\}$.

Setup(λ)：该算法首先选择生成元 $P_1\in G_1$，$P_2\in G_2$ 以及随机数 $a\in Z_N^*$. 计算群 G_1 中的元素 $P_{pub}=aP_1$，群 G_T 中的元素 $g=e(P_{pub},P_2)$. 最后从 G_2 中随机选择 k 个互不相同的元素 $h_1,h_2,\cdots,h_k$，分别对应 k 个不同的属性.

定义系统的主公钥为

$$mpk=\{P_1,P_2,P_{pub},g,h_1,h_2,\cdots,h_k\},$$

主私钥为 $msk=a$.

Encrypt(mpk,M,γ)：该算法输入系统主公钥 mpk，要加密的消息 $M\in\mathbb{G}_{T_2}$，属性集合 S. 选择随机数 $s\in\mathbb{Z}_N^*$，输出密文：

$$ct=(S,C=Mg^s,C'=s(H_1(N)P_1+P_{pub});$$
$$\{C_x=sh_x\}_{x\in S}).$$

KeyGen($mpk,msk,\mathbb{A}$)：该算法输入主密钥 msk 和一个 LSSS 结构的访问策略 $(\boldsymbol{W},\rho)$，其中 $\boldsymbol{W}$ 是一个 $l\times n$ 的矩阵，函数 ρ 将 $\boldsymbol{W}$ 中的行映射到属性集中的属性上. 算法首先选择一个随机的向量 $\boldsymbol{v}=(a,y_2,y_3,\cdots,y_n)\in Z_N^n$，这些值将被用来分享主密钥 a. 其次对于 $i=1$ 到 l，该算法计算 $\lambda_i=\boldsymbol{v}\cdot\boldsymbol{W}_i$，其中 $\boldsymbol{W}_i$ 是矩阵 $\boldsymbol{W}$ 中的第 i 行向量. 最后该算法选择随机值 $r_1,r_2,\cdots,r_l\in Z_N$，输出解密密钥 SK 为

$$D_1=\frac{\lambda_1}{H_1(N)+a}P_2+r_1h_{\rho(1)},$$
$$R_1=r_1(H_1(N)+a)P_1,$$
$$\forall d\in\Gamma/\rho(1),\ Q_{1,d}=r_1h_d$$
$$\cdots$$
$$D_l=\frac{\lambda_l}{H_1(N)+a}P_2+r_lh_{\rho(l)},$$
$$R_l=r_l(H_1(N)+a)P_1,$$
$$\forall d\in\Gamma/\rho(l),\ Q_{l,d}=r_lh_d.$$

这里 Γ 指的是秘密生成矩阵对应的不同属性集合，即 $\Gamma=\{d:\exists i\in[1,l],\rho(i)=d\}$.

Decrypt($mpk,sk_{\mathbb{A}},ct$)：该算法输入与访问策略 $(\boldsymbol{W},\rho)$ 相对应的密钥 SK 和与集合 S 关联的密文 ct. 假如 S 不满足 $(\boldsymbol{W},\rho)$，则输出 $\perp$，否则定义 $I\subset\{1,2,\cdots,l\}$ 且 $I=\{i:\rho(i)\in S\}$，令 $\{\omega_i\in\mathbb{Z}_N|i\in I\}$ 为满足如下条件的常数集合：$\sum_{i\in I}\omega_i\boldsymbol{W}_i=(1,0,0,\cdots,0)$. 注意 ω_i 的选择不唯一，而且这里可能存在多个集合 I 满足上述条件. 定义 $\Delta=\{x:\exists i\in I,\rho(i)=x\}$，它指的是解密时使用的不同属性集合，显然 $\Delta\subseteq S$（S 是加密时使用的属性集合），且 $\Delta\subseteq\Gamma$（Γ 指的是秘密生成矩阵中对应的不同属性集合）. 算法计算如下：

(1) 计算 $L=\sum_{x\in\Delta}C_x=\sum_{x\in\Delta}sh_x=sf(\Delta)$；其中 $f(\Delta)=\sum_{x\in\Delta}h_x$.

(2) 计算

$$D_i'=D_i+\sum_{x\in\Delta/\rho(i)}Q_{i,x}$$
$$=\frac{\lambda_i}{H_1(N)+a}P_2+r_i\left(h_{\rho(i)}+\sum_{x\in\Delta/\rho(i)}h_x\right)$$
$$=\frac{\lambda_i}{H_1(N)+a}P_2+r_if(\Delta).$$

(3) 计算

$$\frac{e\left(C',\sum_{i\in I}w_iD_i'\right)}{e\left(\sum_{i\in I}w_iR_i,L\right)}$$

$$=\frac{e\left(s(H_1(N)P_1+P_{pub}),\sum_{i\in I}w_i\left(\frac{\lambda_i}{H_1(N)+a}P_2+r_if(\Delta)\right)\right)}{e\left(\sum_{i\in I}w_i(r_i(H_1(N)+a)P_1),sf(\Delta)\right)}$$

$$=\frac{e\left(sP_1,\sum_{i\in I}w_i\lambda_iP_2\right)\cdot e\left(s(H_1(N)P_1+P_{pub}),\sum_{i\in I}w_ir_if(\Delta)\right)}{e\left(\sum_{i\in I}w_i(r_i(H_1(N)+a)P_1),sf(\Delta)\right)}$$

$$=e\left(sP_1,\sum_{i\in I}w_i\lambda_iP_2\right)=e(P_1,P_2)^{s\sum_{i\in I}w_i\lambda_i}=e(P_1,P_2)^{sa}=g^s.$$

最后,该算法计算 C/g^s 得到消息 M.

4.2 安全性分析

定理 2. 如果 $(q,k+1)$-DBDHI 假设成立,那么本文提出的改进方案是 IND-SST-CPA 安全的.

证明. 方案的证明同基础方案的证明类似,除了在私钥询问时,模拟者需要对 $\forall d\in\Gamma/\rho(i)$,设置 $Q_{i,d}=r_ih_d$,计算如下:

当 $x\in S^*$ 时,

$$\begin{aligned}Q_{i,d}&=r_ih_d\\&=\left(r_i'-\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)-1}\right)z_x(a+c)Q\\&=r_i'h_d-Ec_i(a+c)^{k+2-\rho(i)}Q,\end{aligned}$$

当 $x\notin S^*$ 时,

$$\begin{aligned}Q_{i,d}&=r_ih_d\\&=\left(r_i'-\frac{Ec_i}{z_x}(a+c)^{k+2-\rho(i)-1}\right)\frac{z_x}{(a+c)^{k+2-d}}Q\\&=r_i'h_d-Ec_i(a+c)^{d-\rho(i)-1}Q,\end{aligned}$$

此时,$d\neq\rho(i)$,所以 $d-\rho(i)-1\neq-1$,从而 $(a+c)^{k+2-\rho(i)}Q$ 可以通过问题实例计算得出.

在重新随机化阶段,模拟者需要对 $\forall d\in\Gamma/\rho(i)$,设置 $Q'_{i,d}=Q_{i,d}+r_i''h_d$.

证毕.

4.3 效率分析

本部分在 256 bit 安全下对基础方案和改进方案的解密效率进行分析与比较. 在改进方案中,解密操作虽然将配对运算数量减少到 2 个,但是增加了大约 $|I|\cdot|\Delta|$ 个 G_2 中的点加运算,而基础方案中解密操作大约需要 $2|I|$ 个配对运算,在一台 Intel(R)i5,64-bit 的 Windows 10 操作系统,16 GB 内存的笔记本电脑中,用 MIRACL 库中的 BN256 曲线,计算一个 R-ate 双线性配对运算大约需要 31 ms,计算一个群 G_2 中的点加运算大约需要 0.15 ms. 假设 $|\Delta|=|I|$,则当 $|\Delta|>413$ 时,改进方案更加耗时,此时我们应该选择基础方案.

4.4 动态自适应的解密操作

相比于基础方案,改进方案的密钥长度和密钥生成时间都扩大了 $|\Gamma|$ 倍,在实际应用中,应该考虑这样的密钥扩张是否值得. 因此,本节提出了一个在私钥长度和解密时间之间进行权衡的方法. 本节首先提出了一个动态自适应的解密操作,然后根据解密操作选择密钥大小.

(1) 动态自适应的解密操作

首先,将第 4.1 节解密时定义的集合 Δ 分解成 y 个互不相交的 $\Delta_i(i=1,2,\cdots,y)$,并定义函数 $w:\Delta\to[1,y]$,使得当 $x\in\Delta_j$ 时,$w(x)=j$,然后对每个 $i\in I$,计算

$$\begin{aligned}D_i'&=D_i+\sum_{x\in\Delta_{w(\rho(i))}/\rho(i)}Q_{i,x}\\&=\frac{\lambda_i}{H_1(N)+a}P_2+r_i\left(h_{\rho(i)}+\sum_{x\in\Delta_{w(\rho(i))}/\rho(i)}h_x\right)\\&=\frac{\lambda_i}{H_1(N)+a}P_2+r_if(\Delta_{w(\rho(i))});\end{aligned}$$

其中 $f(\Delta_{w(\rho(i))})=\sum_{x\in\Delta_{w(\rho(i))}}h_x$.

对于每一个 $j\in[1,y]$,计算

$$L_j=\sum_{x\in\Delta_j}C_x=\sum_{x\in\Delta_j}sh_x=sf(\Delta_j),$$

其中 $f(\Delta_j)=\sum_{x\in\Delta_j}h_x$.

最后计算 $\dfrac{e\left(C',\sum_{i\in I}w_iD_i'\right)}{\prod_{j=1}^{y}e\left(\sum_{i;\rho(i)\in\Delta_j}w_iR_i,L_j\right)}$ 恢复出 g^s.

上述解密过程需要 $(1+y)$ 个配对运算和大约 $|\Delta_1|^2+|\Delta_2|^2+\cdots+|\Delta_y|^2$ 个 G_2 中的点加运算. 特殊的,当 $y=1$ 时,他表示改进方案,当 $y=\Delta$ 时,表示基础方案.

(2) 减小密钥大小

在上述解密操作中,每个 D_i' 的计算仅与 $\Delta_{w(\rho(i))}$ 中的 $Q_{i,x}$ 有关,因此在密钥生成时可以去除那些不在同一个子集 $\Delta_{w(\rho(i))}$ 中的 $Q_{i,x}$,从而减少密钥的长度. 最后该系统的安全性同改进方案的安全性一致,因为该系统中的每个私钥都是改进方案的私钥子集.

4.5 短密文的实现

第 4.1 节的方案更多的是关注解密时间,而对于带宽和存储空间受限的应用设备来说,人们更加

关注密文的大小.因此本节考虑如何实现固定长度的密文.在改进方案的解密算法中,首先使用聚合技术将密文中的 C_x 聚合成 L,因此,在密文中可以直接使用 L 来代替 C_x,从而使密文的大小由原来的 $2+|S|$ 个群元素减少到现在的 3 个群元素.但是相应的代价是与改进方案相比,解密密钥的大小需要扩展到原来的 $|\mathcal{U}|=k$ 倍,而不是 Γ 倍,即在生成解密密钥时,使用$\mathcal{U}$来代替 Γ,这是为了使解密者可以处理任何属性集合的聚合,具体的操作如下

密文结构为

$$ct=(S,C=Mg^{s},\ C'=s(H_1(N)P_1+P_{pub});\ L=\sum_{x\in S}C_x=sf(S)),$$

密钥结构为

$$D_1=\frac{\lambda_1}{H_1(N)+a}P_2+r_1h_{\rho(1)},$$
$$R_1=r_1(H_1(N)+a)P_1,$$
$$\forall d\in\mathcal{U}/\rho(1),\ \mathrm{Q}_{1,d}=r_1h_d$$
$$\cdots$$
$$D_l=\frac{\lambda_l}{H_1(N)+a}P_2+r_lh_{\rho(l)},$$
$$R_l=r_l(H_1(N)+a)P_1,$$
$$\forall d\in\mathcal{U}/\rho(l),\ \mathrm{Q}_{l,d}=r_lh_d$$

显然,此时密钥的大小是 $|\mathcal{U}|\cdot l=k\cdot l$,由于密钥中使用到了属性集合$\mathcal{U}$,因此该方法仅对小属性域的 KP-ABE 有用.最后在解密算法中,虽然用 S 代替了 Δ,增加了群 G_2 中的点加运算,但并不改变配对运算的个数.

5　性能分析

5.1　理论分析

第 5.1 节主要从理论方面评估所提方案的性能,其中 $|G_i|(i=1,2,T)$ 表示群 $G_i(i=1,2,T)$ 中元素的长度,k 代表属性空间大小,$|S|$ 代表加密时使用的属性集合大小,l 代表线性秘密生成矩阵的行数,$|\Gamma|$ 代表秘密生成矩阵对应的不同属性个数,$|I|$ 代表解密时使用的线性秘密生成矩阵中的行数,Δ 代表解密时使用的不同属性集合.表 1 比较了本文的基础方案与改进方案以及文献[4,6,8]中经典快速解密方案的通信开销,结果显示与基础方案相比,改进方案中的私钥长度增加了 $|\Gamma|\cdot l$ 个群 $|G_2|$ 的元素,但是密文长度仅有 3 个群元素.另外,改进方案在系统主公钥、用户私钥和密文上的通信代价上同文献[4]相当,本文方案的公钥长度和私钥长度与文献[6,8]相比通信代价较大,但是本文方案的密文长度只有 3 个群元素,而文献[6,8]的密文长度与加密时使用的属性集合大小成线性关系.

表 1　通信开销比较

方　案	公钥长度	私钥长度	密文长度
基础方案	$\|G_1\|+(k+2)\|G_2\|+\|G_T\|$	$l(\|G_1\|+\|G_2\|)$	$\|G_T\|+\|S\|(\|G_1\|+\|G_2\|)$
改进方案	$\|G_1\|+(k+2)\|G_2\|+\|G_T\|$	$l(\|G_1\|+\|\Gamma\|\|G_2\|)$	$\|G_T\|+\|G_1\|+\|G_2\|$
文献[4]	$(k+1)\|G_1\|+\|G_T\|$	$l(\|\Gamma\|+1)\|G_1\|$	$\|G_T\|+2\|G_1\|$
文献[6]	$3\|G_2\|+2\|G_T\|$	$3(l\|G_1\|+\|G_2\|)$	$\|G_T\|+3(\|S\|+1)\|G_2\|$
文献[8]	$\|G_1\|+\|G_2\|+\|G_T\|$	$l\|G_1\|+\|G_2\|$	$\|G_T\|+\|S\|\|G_1\|+\|G_2\|$

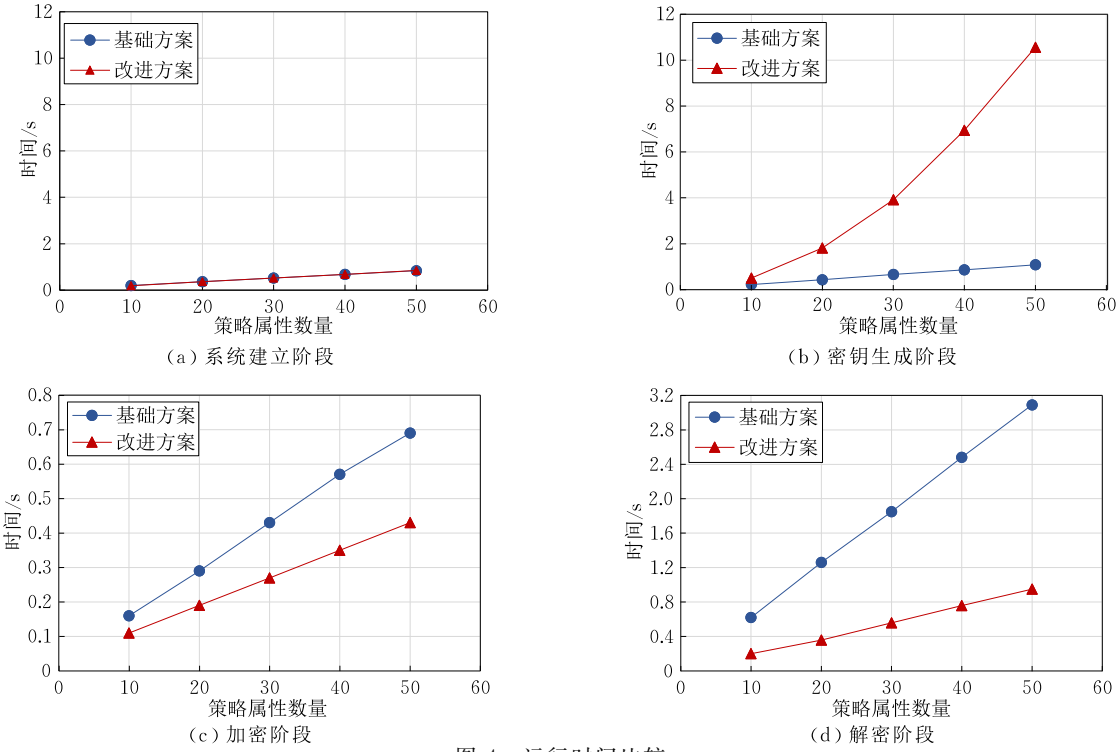
表 2 比较比较了本文的基础方案与改进方案以及文献[4,6,8]中经典快速解密方案的计算开销.我们统一在加法群中定义如下符号并统计计算开销.$sm1$ 代表群 G_1 中的模乘运算,$sm2$ 代表群 G_2 中的模乘运算,T_e,T_i 分别代表群 G_T 中的指数运算和逆运算,T_p 代表一个配对运算.结果显示,与基础方案相比,改进方案在密钥生成阶段增加了 $|\Gamma|\cdot l$ 倍的群 G_2 中的模乘运算.但是,加密操作减少了大约 $|S|$ 倍群 G_1 中的模乘运算,解密操作将配对运算数量由 $2|I|$ 个减少到了 2 个,但是增加了 $|I|\cdot|\Delta|$ 倍的群 G_2 中的模乘运算.第 4.3 节对此进行了详细分析.另外,本文的改进方案与文献[4]的密钥生成算法、加密算法和解密算法的计算代价相当.本文方案中的密钥生成算法与文献[6,8]相比计算代价较大,但是,加密算法与解密算法与文献[6]相比都更加高效,与文献[8]相当.而且本文方案是在 DBDHI 假设下证明安全的,而文献[8]中的方案是在一般的群模型下证明安全的.本文提出的快速解密方法首次验证了基于 SM9 的密钥策略属性基加密方案可以在一定程度上实现快速解密功能,论文接下来的主要工作将是提高基于 SM9 的密钥策略属性基加密方案的整体计算代价和通信代价.

表 2　计算开销比较

方　案	密钥生成	加　密	解　密
基础方案	$l(sm1+2sm2)$	$T_e+\|S\|(sm1+sm2)$	$2\|I\|T_p+T_i$
改进方案	$l(sm1+(\|\Gamma\|+1)sm2)$	$T_e+sm1+\|S\|sm2$	$2T_p+\|I\|(sm1+\|\Delta\|sm2)+T_i$
文献[4]	$l(\|\Gamma\|+2)sm1$	$T_e+(\|S\|+1)sm1$	$2T_p+2\|I\|sm1+T_i$
文献[6]	$(9nl+3l)sm1+3sm2$	$2T_e+6\|S\|sm1+3sm2$	$6T_p+6\|I\|sm1+T_i$
文献[8]	$2lsm1+sm2$	$T_e+\|S\|sm1+sm2$	$2T_p+2\|I\|sm1+T_i$

5.2 实验分析

为了与现有使用 SM9 的信息系统有效融合，本节在 256 bit 安全下使用与 SM9 标识加密相同的 R-ate双线性配对运算和 BN 曲线对所提基础方案和改进方案进行编程仿真，测试方案中每个子算法的运行时间. 测试中使用的设备是一台具有如下参数的笔记本电脑：Intel(R) Core(TM) i5-11300H @3.10 GHz，3.11 GHz CPU，64-bit Windows 10 操作系统，16.0 GB 内存. 测试使用的编程语言是 C++，使用的密码学库是 Miracl (Multiprecision Integer and Rational Arithmetic C/c++ Library. 为了模拟最坏的情况，"'S_1' AND 'S_2' AND … 'S_n'"将作为与解密密钥相关的访问策略，其中 S_i 代表一个属性. 为了保障数据的准确性，本文设置了 5 种不同的策略属性数量，分别是 $n=10,20,30,40,50$，并设置系统属性空间大小为策略属性数量的 2 倍，即属性空间大小分别为 $k=20,40,60,80,100$. 对于每种情形($(n=10,k=20)$,$(n=20,k=40)$,$(n=30,k=60)$,$(n=40,k=80)$,$(n=50,k=100)$)，本文分别设置了 10 组不同的具体属性. 因此，本文总共设置了 50 种不同的访问策略，对于每种访问策略，重复运行 30 次，然后取平均值. 通过比较基础方案与改进方案中各个子算法的运行时间来评估本文改进方案的效率. 图 4(a)说明本文的改进方案与基础方案在系统建立阶段的运行时间是一样的，图 4(b)表明改进方案在密钥生成阶段相比于基础方案较耗时，图 4(c)和图 4(d)说明了改进方案在加密阶段和解密阶段都更加高效. 当策略属性数量为 50，改进方案中的加密操作仅用时 0.43 s，解密操作仅用时 0.95 s，与基础方案中的 3.09 s 相比，解密时间缩短了至少 69.2%①. 实验结果与理论分析结果一致.



(a) 系统建立阶段　(b) 密钥生成阶段

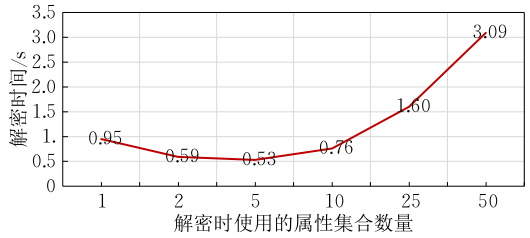
(c) 加密阶段　(d) 解密阶段

图 4　运行时间比较

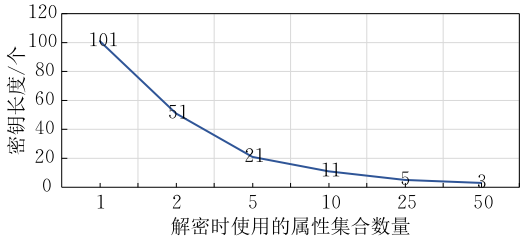
为了验证本文所提出的快速解密方法可以实现动态自适应的解密操作，取其中一种策略属性数量进行实验说明，即策略属性数量 $n=50$，属性空间大小 $k=100$. 设置解密时将集合 Δ 分解成的属性集合数量分别为 $y=1,2,5,10,25,50$，验证解密时使用的不同属性集合数量对解密时间和解密密钥长度的影响. 根据 SM9 标识加密，$|G_2|=2|G_1|$，因此，解密密钥的长度统一用 $|G_1|$ 来表示. 由于策略属性数量 $n=50$，每种情况下统计解密密钥的长度都需要乘以 50. 对此，本文使用 $50|G_1|$ 为单位来统计解密密钥的长度. 实验结果如图 5 所示，当解密时使用的属性集合数量越大时，解密时间一般越长②，但是解

① 在实验模拟中，我们假设 $|S|=|I|=l=n$，但是在实际应用中，$|S|\geq|I|$，此时，解密时间的缩短比例将更高.

② 当 $y=2$ 和 $y=5$ 时，解密时间出现变短现象. 因为当解密时使用的属性集合数量变为 $y=2$ 和 $y=5$ 时，虽然相比于 $y=1$ 时增加了一些配对运算，但是减少了大量群 G_2 中的点加运算. 而当 $y=10$ 时，增加了大量的配对运算，而减少了少量群 G_2 中的点加运算，解密时间变长. 总体的变化趋势是解密时使用的属性集合数量越大，解密时间一般越长.



(a) 解密时间与解密时使用的属性集合数量关系



(b) 密钥长度与解密时使用的属性集合数量关系

图 5　解密时间与密钥长度的权衡

密密钥的长度越短. 在实际应用中，可以根据不同需求选择不同的参数.

为了测试第 4.5 节提出的具有短密文的基于SM9的密钥策略属性基加密快速解密方法的基本性能. 本实验同样在策略属性数量 $n=10,20,30,40,50$，属性空间大小 $k=20,40,60,80,100$ 时，进行仿真测试. 如上述实验所示，同样假设 $|S|=|\Delta|=|I|=n$. 由第 4.5 节的理论分析知，该方法同 4.1 节的快速解密方法在系统建立和数据加密阶段使用的运算都基本相同. 在解密阶段，该方法使用 S 代替 Δ，仅增加了群 G_2 中的点加运算，并没有改变配对运算的个数. 因此，在上述假设下，该方法同第 4.1 节快速解密方法的解密操作耗时相当. 本节主要比较两种方法的密钥生成时间. 实验结果如图 6 所示，在上述假设下，具有短密文的基于 SM9 的密钥策略属性基加密的密钥生成时间大约是第 4.1 节快速解密方法的 2 倍. 实验结果与理论分析一致.

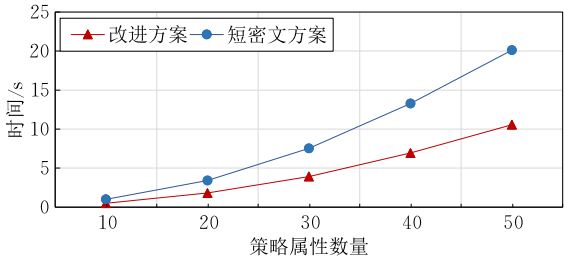


图 6　密钥生成时间比较

6　总结与展望

针对标识密码 SM9 标识加密不能满足分布式计算系统对数据的细粒度访问控制功能，本文在 SM9 标识加密的基础上，利用 LSSS 构造了一种 KP-ABE 方案，并在 $(q,k+1)$-DBDHI 假设下证明了方案满足 IND-SST-CPA 安全性. 在此基础上，本文也提出了一种基于 SM9 的 KP-ABE 快速解密方法，该方法将解密时使用的双线性配对运算数量减少至 2 个，密文长度减少至 3 个群元素. 理论分析和实验仿真表明：相比于基础方案，本文的快速解密方法可以将解密时间减少至少 69.2%. 未来工作将致力于在实现 SM9 密钥策略属性基加密快速解密和定长密文的前提下，最大限度地减少解密密钥所带来的计算开支和通信开销.

致　谢　衷心感谢编辑们和评审专家们对本文提出的宝贵意见和建议！

参　考　文　献

[1] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[2] Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption//Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography. Paris, France, 2010: 19-34

[3] Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 90-108

[4] Hohenberger S, Waters B. Attribute-based encryption with fast decryption//Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography. Nara, Japan, 2013: 162-179

[5] Lai J, Deng R H, Li Y, et al. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption//Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. Kyoto, Japan, 2014: 239-248

[6] Agrawal S, Chase M. FAME: fast attribute-based message encryption//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 665-682

[7] Kumar N, Samriya J K. Secure data validation and transmission in cloud and IoT through ban logic and KP-ABE. International Journal of Sensors Wireless Communications and Control, 2022, 12(1): 79-87

[8] Riepel D, Wee H. FABEO: Fast attribute-based encryption with optimal security//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles, USA, 2022: 2491-2504

[9] Hafizpour H, Shiri M E, Rahmani A M. New attribute-based encryption schemes with anonymous authentication and time limitation in fog computing. Concurrency and Computation: Practice and Experience, 2023: e7681

[10] Jain A, Lin H, Luo J. On the optimal succinctness and efficiency of functional encryption and attribute-based encryption//Proceedings of the 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lyon, France, 2023: 479-510

[11] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts//Proceedings of the 20th USENIX Security Symposium. San Francisco, USA, 2011: 523-538

[12] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: Verifiable computation from attribute-based encryption//Proceedings of the 9th Theory of Cryptography Conference. Taormina, Italy, 2012: 422-439

[13] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354

[14] Zhang K, Gong J, Tang S, et al. Practical and efficient attribute-based encryption with constant-size ciphertexts in outsourced verifiable computation//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Xi'an, China, 2016: 269-279

[15] Sun Yi, Chen Xing-Yuan, Du Xue-Hui, et al. Dynamicauthenticated method for outsourcing data stream with access-control in cloud. Chinese Journal of Computers, 2017, 40(2): 337-350(in Chinese)
(孙奕, 陈性元, 杜学绘等. 一种具有访问控制的云平台下外包数据流动态可验证方法. 计算机学报, 2017, 40(2): 337-350)

[16] Ning J T, Cao Z F, Dong X L, et al. Auditableσ-time outsourced attribute-based encryption for access controlin cloud computing. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 94-105

[17] Yang W T, Wang R M, Guan Z T, et al. A lightweight attribute based encryption scheme with constant size ciphertext for Internet of Things//Proceedings of the 2020 IEEE International Conference on Communications. Dublin, Ireland, 2020: 1-6

[18] Astudillo K. Multi-User Searchable Attribute-Based Encryption for Outsourced Big Data for Create, Update, Read and Delete Operations [Ph. D. dissertation]. California State University, Northridge, 2023

[19] Cheng Z. Security analysis of SM9 key agreement and encryption //Proceedings of the 14th International Conference on Information Security and Cryptology. Fuzhou, China, 2018: 3-25

[20] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. Security analysis of SM9 digital signature and key encapsulation. Science China: Information Sciences, 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)

[21] Qin Bao-Dong, Zhang Bo-Xin, Bai Xue. 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. 基于仲裁的 SM9 标识加密算法. 计算机学报, 2022, 45(2): 412-426)

[22] 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)

[23] Tang Fei, Ling Guo-Wei, Shan Jin-Yong. Additive homomorphic encryption schemes based on SM2 and SM9. Journal of Cryptologic Research, 2022, 9(3): 535-549(in Chinese)
(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)

[24] Pu Lang, Lin Chao, Wu Wei, et al. A public-key encryption with keyword search schemefrom SM9. Journal of Cyber Security, 2023, 8(1): 108-118(in Chinese)
(蒲浪, 林超, 伍玮等. 基于 SM9 的公钥可搜索加密方案. 信息安全学报, 2023, 8(1): 108-118)

[25] Gan Zhi-Wang, Liao Fang-Yuan. Rapid calculation of R-ate bilinear pairing in China state cryptography standard SM9. Computer Engineering, 2019, 45: 171-174(in Chinese)
(甘植旺, 廖方圆. 国密 SM9 中 R-ate 双线性对快速计算. 计算机工程, 2019, 45: 171-174)

[26] Wang Ming-Dong, He Wei-Guo, Li Jun, et al. Optimal design of R-ate pair in SM9 algorithm. Communications Technology, 2020, 53: 2241-2244(in Chinese)
(王明东, 何卫国, 李军等. 国密 SM9 算法 R-ate 对计算的优化设计, 通信技术, 2020, 53: 2241-2244)

[27] Shamir A. Identity-based cryptosystems and signature schemes// Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Santa Barbara, USA, 1984: 47-53

[28] Koblitz N. Introduction to Elliptic Curves and Modular Forms. Berlin: Springer, 1984: 375-384

[29] Miller V. Use of elliptic curves in cryptography//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Santa Barbara, USA, 1985: 417-426

[30] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the International Cryptology Conference. Santa Barbara, USA, 2001: 213-229

[31] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland, 2003: 255-271

[32] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland, 2004: 223-238

[33] Waters B. Efficient identity-based encryption without random oracles//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 114-127

[34] Döttling N, Garg S. Identity-based encryption from the Diffie-Hellman assumption//Proceedings of the 37th Annual International Cryptology Conference. Santa Barbara, USA, 2017: 537-569

[35] Cheng Z. The SM9 cryptographic schemes. Cryptology ePrint Archive, 2017: 117

[36] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457-473

[37] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 2007 IEEE Symposium on Security and Privacy. Oakland, USA, 2007: 321-334

[38] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute based encryption//Proceedings of the 35th International Colloquium on Automata, Languages and Programming. Reykjavik, Iceland, 2008: 579-591

[39] Attrapadung N, Imai H. Attribute-based encryption supporting direct/indirect revocation modes//Proceedings of the 12th IMA International Conference on Cryptography and Coding, Cirencester, UK, 2009: 278-300

[40] Ibraimi L, Tang Q, Hartel P, et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes//Proceedings of the 5th International Conference on Information Security Practice and Experience. Xi'an, China, 2009: 1-12

[41] Shi Y, Ma Z Y, Qin R F, et al. Implementation of an attribute-based encryption scheme based on SM9. Applied Sciences, 2019, 9(15): 3074

[42] Ji H H, Zhang H J, Shao L S, et al. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. Connection Science, 2021, 33(4): 1094-1115

[43] Fujisaki E and Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Proceedings of the 19th Annual International Cryptology Conference. Santa Barbara, USA, 1999: 537- 554

[44] Lai Jian-Chang, Huang Xin-Yi, He De-Biao, et al. An efficient hierarchical identity-based encryption based on SM9. Science China: Information Sciences, 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)

[45] Beimel A. Secure schemes for secret sharing and key distribution. Israel Institute of Technology, Haifa, Israel, 1996

LIU Xiao-Hong, Ph. D. Her research interests include cryptography and information security.

HUANG Xin-Yi, Ph. D., associate professor. His research interests include cryptography and artificial intelligence.

CHENG Zhao-Hui, Ph. D. His research interests include cryptography and data security.

WU Wei, Ph. D., lecturer. Her research interests include cryptography and information security.

Background

This article delves into the realm of Key-Policy Attribute-Based Encryption (KP-ABE) based on SM9, which is aseries of Identity-Based Cryptosystem (IBC) algorithms designed by our country, including digital signature algorithm, key exchange protocol, key encapsulation mechanism and public key encryption algorithm. So far, SM9 has become a national and international standards. Although SM9 has been used in many fields, effectively ensure the national network and information security. However, it is designed to meet the basic security requirements of network and information systems, that is, to ensure the confidentiality and integrity of data. For this reason, many scholars have carried out extensive research on SM9, including security analysis and functional extension. For instance, some studies have focused on designing broadcast encryption, searchable encryption, and semi-homomorphic encryption algorithms based on SM9. ABE is classified among the most promising cryptographic primitives derived from Identity-Based Encryption (IBE). In

2005, based on IBE, Sahai and Waters first proposed the prototype of ABE concept, namely Fuzzy Identity-Based Encryption (FIBE). In 2006, Goyal et al. refined the idea of ABE into two complementary types: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), and propose the first KP-ABE scheme. In KP-ABE, the private key is linked to an access policy, while the ciphertext is linked to an attribute set. The decryption would be successful if and only if the set of attributes connected to the ciphertext satisfies the access policy related to the private key. CP-ABE is just the opposite. In 2007, Bethencourt et al. proposed the first CP-ABE scheme. Since then, many researchers have conducted extensive research on FIBE, KP-ABE, and CP-ABE. However, all these algorithms are designed based on the foreign IBE, and so far, there are no existing KP-ABE algorithms based on SM9.

In this paper, we propose the first KP-ABE based on SM9 using Linear Secret Sharing Scheme (LSSS) and its fast decryption method. Our proposed schemes mainly have the following characteristics: (1): finer-grained access control; (2) fast decryption; (3) constant-size ciphertext; (4) dynamic adaptability. In addition, we also prove the security of the proposed schemes under the $(q, k+1)$-DBDHI difficult problem assumption. Theoretical analysis and experimental simulation show that the fast decryption method proposed in this paper can reduce the decryption time by at least 69.2%. Moreover, it is comparable to the classical fast decryption methods in terms of computing cost and communication cost, and is feasible in practical application.

This work is supported by the Foundation: National Natural Science Foundation of China under Grant Nos. 62032005 and 62372108.