支持等式测试的身份基可否认认证加密方案及其在电子投票系统的应用

姚天昂[1,2,3], 熊 虎[1,2]

[1] 电子科技大学信息与软件工程学院 成都 中国 610054
[2] 网络与数据安全四川省重点实验室(电子科技大学) 成都 中国 610054
[3] 南京大学计算机科学与技术系 南京 中国 210023

摘要 电子投票系统被认为是现代生活中高效提供政府服务和进一步加强民主活力的方法。但是, 现有构建电子投票系统的方法存在以下问题: 第一, 在面临贿选及胁迫的压力时, 选民无法无视外在压力独立投票。其次, 审计投票结果的实体可以在审计的同时获知有关投票内容的额外信息。为了解决上述两个问题, 我们首次将可否认认证加密技术与身份基等式测试加密技术相结合, 提出了一种支持等式测试的身份基可否认认证加密方案。该方案可以在第三方服务器不解密的情况下提供密文可比性, 还能保证接收方验证发送方的身份的同时, 不能向第三方证明信息来自发送方, 从而保护发送方的隐私。该方案利用可否认认证加密技术在技术层面保证了选民独立投票的能力, 并额外增加了身份基下的等式测试功能以确保审计机构在逻辑结构上拥有访问权限。在使用本方案的电子投票系统中, 审计机构在审计投票结果的同时, 不获得有关选票的任何其他信息。我们证明了我们的方案在随机预言模型中是安全的, 并且可以在电子投票系统中确保不可胁迫性和可审计性。该方案与已有相关方案相比, 在开销和安全性能均有较好表现的同时, 实现了更为丰富的功能。此外, 我们使用所提出的密码学方案设计了一个安全的电子投票系统, 其安全特性可以很好地保护电子投票系统中的选民自由和公平性。

关键词 电子投票; 不可胁迫性; 可审计性; 可否认认证加密; 身份基密码体制; 等式测试
中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.09.08

Identity-based deniable authenticated encryption with equality test and its application to e-voting system

YAO Tianang[1,2,3], XIONG Hu[1,2]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[2] Network and Data Security Key Laboratory of Sichuan Province(University of Electronic Science and Technology of China), Chengdu 610054, China
[3]Department of Computer Science and Technology Nanjing University, Nanjing 210023, China

Abstract E-voting is considered an approach to further strengthen the provision of government services and the vibrancy of democracy effectively in modern life. However, the existing methods to build an e-voting system have the following issues: First, when facing the pressure of vote-buying and extortion, voters may have no way to cast their votes alone, under no pressure. Second, the entities who can audit the voting results may learn additional information about the content of the ballot during the audit phase. To handle the above two issues, we first integrated the functionalities called deniable authenticated encryption and identity-based encryption with equality test, and we have proposed an identity-based deniable authenticated encryption with equality test scheme (IB-DAE-ET). This scheme not only can provide ciphertext comparability without decryption executed by the third-party server, and can also ensure that the receiver cannot prove to the third party that the information comes from the sender while verifying the identity of the sender. Hence, our scheme is able to protect the sender's privacy. This novel scheme utilizes deniable authenticated encryption to technically guarantee the ability of voters to vote independently, and we add the primitive called identity-based encryption with equality test to ensure audit agencies have logical access to audit the voting results. In e-voting systems that apply this scheme, the audit institution does not obtain any other information about the ballot while auditing the voting results. We prove that our scheme is secure in the random oracle model and can ensure uncoercibility and accountability in the e-voting system. Compared with the existing related schemes, this scheme achieves more abundant functionalities while having better performance in overhead and security properties. Furthermore, we design a secure e-voting system using the proposed deniable authenticated encryption with equality test scheme, which properties can guarantee the freedom and fairness of the e-voting system.

通讯作者: 熊虎, 博士, 教授, Email: xionghu.uestc@gmail.com。
本课题得到国家自然科学基金(No. U1936101, No. 61902054)资助。
收稿日期: 2022-02-05; 修改日期: 2022-04-11; 定稿日期: 2023-06-12

Key words electronic voting; uncoercibility; accountability; deniable authenticated encryption; identity-based cryptography; equality test

1 引言

1.1 研究背景

在过去, 人们通常通过邮件或线下集会进行投票选举心仪的参选者, 现在人们则可以利用互联网在线上使用电子投票系统来完成投票。电子投票是一种采用电子设备进行投票并统计的投票方式。与传统投票方式相比, 采用电子投票可以提升选民的参与度、在投票时间和地点方面为选民提供更多的便利、节约经费和具有更高的准确性[1]。

电子投票还同时具有机密性和可认证性, 其工作流程大致如下: 选民将自己的身份信息和选票内容加密后发送给计票者。计票者会解密选票并验证其是否来源于有效的选民, 然后再将加密的有效选票发送给审计机构。除了选民和计票者以外无法得知每张选票的具体内容。尽管电子投票较之传统投票具有很多优势, 但是还存在一些问题需要解决[2]。首先, 电子投票需要满足不可胁迫性。不可胁迫性是指选民在受到威胁时仍然可以不受干扰地继续坚持自己的投票结果。由于在一次投票中可能存在一个可以控制计票者 Bob 的第三方 Mallory。Mallory 的意图是将选民 Alice 票投给他指定的候选人。如果电子投票系统中没有合适的选民保护机制, Mallory 可以强迫 Bob 交出 Alice 的投票结果从而达到胁迫的目的。因此, 开发一种允许选民在不受任何第三方胁迫的情况下行使他们权利的技术对设计安全的电子投票系统至关重要[3-4]。

上述方案在不完全安全的应用场景中很难保证选民抵抗外部胁迫。因此, 电子投票系统不仅要保证计票者能验证选民的身份, 还需要从技术层面让选民在受到胁迫时可以否认自己的投票结果, 从而保护选民的隐私。一种名为可否认认证协议的密码学原语可以很好地解决上述问题。1998 年, Dwork 等人[5]使用零知识证明构造了一个可否认认证协议。

除了需要满足不可胁迫性, 可审计性也是电子投票系统的需求。可审计性是指所有选民的投票信息都要被第三方数据库相应地记录, 但参与审计的第三方服务器在记录投票信息时不能解密投票信息。传统加密方式可能会限制审计机构对加密的投票信息的搜索和审核能力。如果使用传统加密方式, 审计机构在不知道私钥的情况下用户无法对加密数据进行检索或分类。支持等式测试的公钥加密方案成为了实现可审计性的关键技术。Yang 等人[6]首次提出了支持等式测试的公钥加密方案。该方案允许第三方服务器在两个密文间进行等式测试来判断其是否包含同一个明文。支持等式测试的公钥加密作为一种新的加密原语吸引了许多研究者的注意。

1.2 相关工作

本方案的相关工作主要有支持等式测试的公钥加密, 可否认认证协议和身份基加密机制。

为了实现在加密数据上的检索, Song 等人[7]首次提出了一种名为可搜索加密的密码学原语。该原语利用对称加密技术, 在保护用户数据的机密性的同时可以支持加密数据搜索。但是对称可搜索加密方案并不适用于多用户环境, 原因在于接收方为了保证搜索功能会存储大量不同的对称密钥, 这带来了很大的存储开销。Boneh 等人[8]提出了支持关键词检索的公钥加密的概念。该方案与 Song 等人[7]的方案的不同之处在于使用了公钥密码体制构造可搜索加密方案, 用户不需要存储大量的对称密钥, 只需要保存自己的私钥用于解密和创建搜索陷门进行搜索。但公钥可搜索加密无法在由不同公钥加密生成的密文中进行分类与搜索。为了解决上述问题, Yang 等人[6]首次提出了支持等式测试的公钥加密方案。该方案允许第三方服务器在由不同公钥生成的两个密文间进行等式测试, 从而判断其是否由同一个明文加密得到。值得注意的是, 任何人都可以使用等式测试方法去测试两个密文。在 Yang 等人[6]的方案被提出后, 一些具有认证功能的等式测试方案开始涌现。具有认证功能的方案只允许由发送方指定或被认证身份的测试者进行等式测试。Tang[9]提出了细粒度授权公钥加密的概念, 服务器只能在获得由接收方共同生成的陷门后才能进行等式测试, 这提升了等式测试方案的安全性。Ma 等人[10]提出了支持灵活授权的等式测试方案, 该方案支持四种授权协议以满足用户在不同场景下的需求。Xu 等人[11]继续研究了灵活授权的等式测试方案, 并提出了可验证的支持等式测试的公钥加密方案。该方案给用户提供了验证能力, 即用户可以验证第三方服务器是否诚实地执行了等式测试。Huang 等人[12]提出了具备过滤功能的等式测试方案, 过滤功能指的是只有部分由接收方指定的密文可以进行等式测试。Qu 等人[13]首次提出了支持无证书加密体制的等式测试方案。该方案将无证书公钥加密和等式测试相结合, 同时解决了

密钥托管和证书管理问题。

可否认认证协议作为保证不可胁迫性的重要技术, 近年来发展迅速。Dwork 等人[5]首先使用零知识证明构造了可否认认证协议, 但是该方案的认证过程有较长的时延。Deng 等人[14]提出了两种可否认认证协议, 其中一个是基于大数分解困难问题, 另一个是基于大型有限域上的离散对数困难问题。然而 Deng 等人[14]的方案需要由发送方和接收方共同信任的公共字典。为了避免依赖可信第三方, Fan 等人[15]提出了一种基于 Diffie-Hellman 算法[16]的可否认认证协议。但是此方案的设计过于简单, 且存在一定的安全缺陷, 后续研究多以此协议为模板进行改进。其后, Yoon 等人[17]指出了 Fan 等人[15]的方案在认证方面的不足, 即攻击者可以伪装成发送方所期望的接收方, 且第三方可以很容易地识别伪造消息的真正来源。因此, Yoon 等人[17]提出了一种借助认证机构的可否认认证协议。Shao[18]基于通用 Elgamal 签名方法[19]构造了新的非交互式可否认认证协议, 并证明了只有在在 Elgamal 协议可以被伪造的情况下, 该认证协议才会被攻击者伪造。Lu 等人[20]基于大数分解困难问题提出了一个非交互式可否认认证协议, 并在随机预言模型中证明其安全性。Wang 等人[21]提出了一种基于 ElGamal 算法[22]的可否认认证协议, 该协议不仅结构简单, 而且可以抵抗中间人攻击。Harn 和 Ren[23]设计了一种应用于在电子邮件系统的可否认认证协议。该方案是由发送方直接对密文进行签名, 而不是通过消息摘要进行签名, 这使得签名可被伪造从而实现了完全可否认性。Wang 等人[24]提出了一种基于指定验证者的非交互式可否认认证协议, 并证明其安全。Li 等人[25]在原有协议基础上, 第一次提出了可否认加密方案。该方案可以在逻辑上一步满足机密性和可否认认证, 比以往的方案更为高效。其后, Jin 等人[26]设计了异构的可否认加密方案, 该方案可以提供批量验证功能, 适用于电子投票系统。

早在 1984 年, Shamir[27]就设想了一种公钥密码系统, 其中的公钥可以是任意字符串。该公钥密码系统即为身份基加密系统。身份基加密系统可以减轻公钥密码系统中证书管理的压力。Boneh 等人[28]基于 Weil Pairing 构造了一个身份基加密方案, 并证明其安全。Abdalla 等人[29]首先将身份基加密与公钥可搜索加密相结合, 提出了基于身份基的可搜索加密方案。此外, Abdalla 等人[29]还设计了一种可以将阶级式匿名身份基加密方案变换为身份基可搜索加密方案的通用转换。Ma[30]还提出了基于身份加密的等式测试方案。该方案首次将身份基密码体制与等式测试功能相结合, 解决了原先公钥系统下等式测试方案的证书管理问题。

1.3 本文贡献

为了同时实现电子投票系统的不可胁迫性和可审计性, 本文使用密码学原语来解决上述问题。我们首次将可否认认证协议与支持等式测试的身份基加密方案相结合, 提出了基于身份基的支持等式测试的可否认加密方案(Identity-based Deniable Authenticated Encryption with Equality Test, IB-DAE-ET)。与已有方案相比, 我们的方案贡献如下:

(1) 形式化给出了选择身份与密文攻击下的单向性、选择身份与密文攻击下的不可区分性和选择身份与消息下的可否认认证性的定义和安全模型;

(2) 利用双线性映射给出了方案的具体构造, 并将方案规约到数学困难问题以证明其安全性;

(3) 从理论和实验两部分给出了性能比较和安全性比较, 在扩展了功能的前提下本方案仍然保证了较高的效率。

1.4 章节安排

文章的剩余章节安排如下: 第二章我们主要介绍电子投票系统模型和复杂性假设; 第三章我们会提供 IB-DAE-ET 方案的模型, IB-DAE-ET 原语所包含的基本算法, 安全模型以及方案的具体内容, 并详细地给出了安全性证明; 第四章我们从理论分析和具体实验两方面对本方案进行了比较; 第五章我们利用所提方案设计了一个安全的电子投票系统; 最后一章我们总结了本方案的实际意义, 并对未来研究方向进行了展望。

2 预备知识

在本章节中, 我们会给出本方案适用的电子投票系统模型及本方案依赖的数学困难问题。

2.1 系统模型

该系统模型包含了选民、计票者和审计机构。首先, 计票者将认证方法和投票的内容公布给选民。选民将自己的身份认证信息和选票具体内容加密后发送给计票者。计票者会解密选票并验证其是否有效, 然后将加密状态的有效选票发送给审计机构。最后, 审计机构在不解密选票的状态下存储选票并统计选票信息。图 1 展示了电子投票系统的模型。

2.2 双线性映射

设 G_1 和 G_2 是两个阶为 q 的循环群, g 是 G_1 的生成元。当且仅当映射满足下列性质时, $G_1 \times G_1 \to G_2$ 为一个双线性映射:

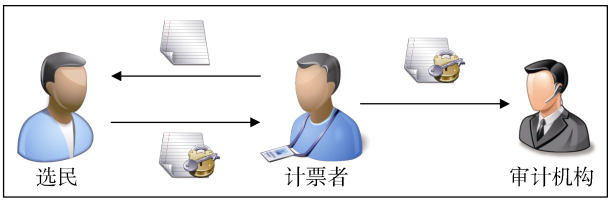


图 1　电子投票系统模型

Figure 1　The system model of e-voting system

(1) 双线性: 对于任意的 $a,b\in Z_p$ 与任意的 $g\in G_1$, $e(g^a,g^b)=e(g,g)^{ab}$;

(2) 非退化性: $e(g,g)\neq 1$;

(3) 可计算性: 对于任意的 $g\in G_1$, 在多项式时间内可以计算出 $e(g,g)$ 的结果。

2.3　双线性 Diffie-Hellman 问题 (Bilinear Diffie-Hellman Problem, BDH)

设 G_1 和 G_2 是两个阶为 q 的循环群, g 是 G_1 的生成元, $e:G_1\times G_1\to G_2$ 为一个双线性映射。在 (q,G_1,G_2,e) 中的 BDH 困难问题如下: 在随机选取 $a,b,c\in Z_q^*$, 并给定 g,g^a,g^b,g^c 时, 任意一个敌手 $\mathcal{A}$ 在多项式时间内计算 $e(g,g)^{abc}$ 时有优势:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{BDH}}\overset{\mathrm{def}}{=}\Pr[\mathcal{A}(g,g^a,g^b,g^c)=e(g,g)^{abc}] \quad (1)$$

如果对于任意多项式时间内的敌手 $\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{BDH}}$ 都是可忽略的量, 我们认为 BDH 困难问题成立。

3　IB-DAE-ET 方案

在 IB-DAE-ET 方案中, 有以下 5 个实体: 发送方、接收方、私钥生成机构、云服务器和某第三方, 图 2 为该方案的系统模型。私钥生成机构生成发送方和接收方的私钥并发送给对应实体。发送方首先使用接收方的公开身份信息与发送方的私钥来加密需要发送的敏感信息, 并将其存储到云服务器上。接收方可以使用自己的私钥和发送方的公开身份来解密密文, 并验证其来源。如果接收方希望委托云服务器进行等式测试, 他可以使用自己的部分私钥生成陷门发送给云服务器来执行等式测试, 而不需要给予云服务器解密能力。此外, 接收方可以验证发送方的身份, 但不能向第三方证明信息来自发送方, 从而保护发送方的隐私。

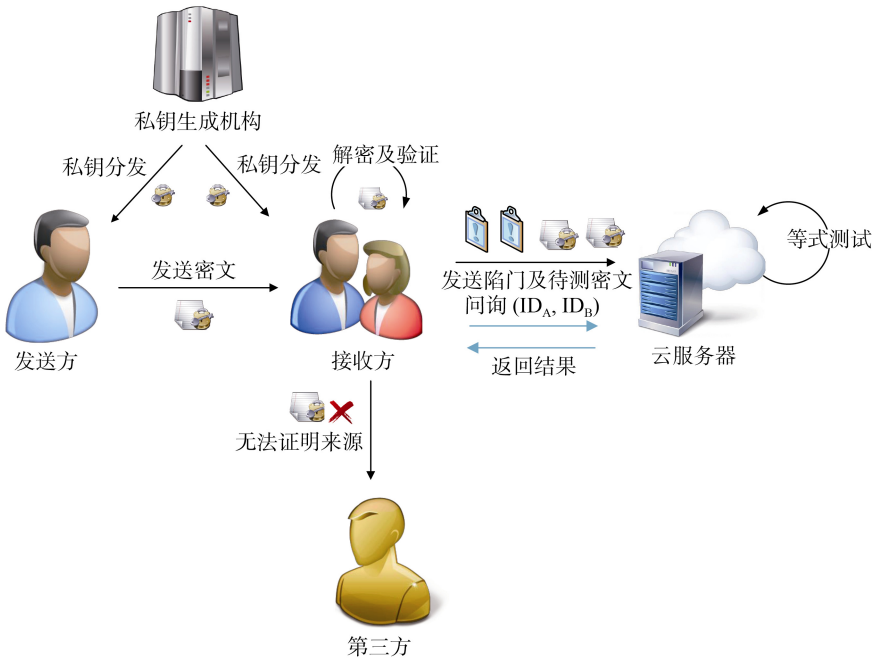


图 2　The system model of IB-DAE-ET scheme

Figure 2　IB-DAE-ET 系统模型

IB-DAE-ET 方案包含以下 6 个算法:

Setup: 用户输入安全参数 λ, 输出系统参数 $Param$ 和主密钥 msk。

ExtractKey: 用户输入 msk 和任意一个身份 ID, 输出对应此身份 ID 的私钥 sk。

Trapdoor: 输入接收方的身份 ID_r, 输出该接收方的陷门 td_r。

DA-Encrypt: 输入明文 M, 发送方的身份 ID_s 和接收方的身份 ID_r, 然后运行本算法, 生成密文 CT。

DA-Decrypt：输入密文 CT，接收方的私钥 sk_r 和发送方的身份 ID_s，然后运行本算法，如果解密结果为有效密文，输出解密结果 M，否则返回错误 $\perp$。

Test：输入用户 i 的密文 CT_i，对应陷门 td_i，和用户 j 的密文 CT_j，对应陷门 td_j，运行本算法。如果返回 1，说明 CT_i 和 CT_j 由相同的明文加密得到。否则返回 0，说明 CT_i 和 CT_j 不是来源于相同的明文。

3.1 IB-DAE-ET 安全模型

DA-IBE-ET 方案定义了 3 种类型的敌手，这些敌手对应了 3 种不同的安全模型，即选择身份与密文攻击下的单向性(One-wayness under chosen identity and chosen ciphertext attacks, OW-ID-CCA)，选择身份与密文攻击下的不可区分性(Indistinguishability under chosen identity and chosen ciphertext attacks, IND-ID-CCA)和选择身份与消息攻击下的可否认认证性(Deniable authentication against chosen identity and message attacks, DA-ID-CMA)。

3.1.1 选择身份与密文攻击下的单向性(OW-ID-CCA)

本方案的 OW-ID-CCA 安全模型通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}_1$ 之间的安全游戏进行定义，该安全游戏描述如下:

第一类敌手 $\mathcal{A}_1$：第一类敌手拥有接收方的陷门，该类型敌手的目的是通过挑战密文恢复出明文。

初始化： 挑战者 $\mathcal{C}$ 将安全参数 λ 作为输入，运行 Setup 算法生成系统参数 $Param$ 并将其传递给 $\mathcal{A}_1$，并生成主密钥 msk 由自己保管。

问询阶段 1： $\mathcal{A}_1$ 可以以任意顺序多次进行以下询问:

私钥提取询问：$\mathcal{A}_1$ 询问与身份 ID_u 相关的私钥，$\mathcal{C}$ 运行 ExtractKey 算法并返回对应的私钥 sk_u 给 $\mathcal{A}_1$。

陷门询问：$\mathcal{A}_1$ 询问与身份 ID_u 相关的陷门，$\mathcal{C}$ 运行 Trapdoor 算法生成陷门 td_u 并发送给 $\mathcal{A}_1$。

可否认认证加密询问：$\mathcal{A}_1$ 选择明文 M，发送方身份 ID_s 与接收方身份 ID_r 提交给 $\mathcal{C}$。$\mathcal{C}$ 首先运行 ExtractKey 获得发送方的私钥 sk_s，再运行 DA-Encrypt 生成密文 CT，并将 CT 返回给 $\mathcal{A}_1$。

可否认认证解密询问：$\mathcal{A}_1$ 选择密文 CT 和接收方身份 ID_r 提交给 $\mathcal{C}$。$\mathcal{C}$ 首先运行 ExtractKey 获得接收方的私钥 sk_r，再运行 DA-Decrypt 生成明文 M。若 M 是有效密文，则返回给 $\mathcal{A}_1$，否则返回错误 $\perp$。

挑战阶段： $\mathcal{A}_1$ 结束问询阶段 1，选择没有进行过私钥提取询问的发送方身份 ID_s^* 和接收方身份 ID_r^* 并发送给挑战者 $\mathcal{C}$。$\mathcal{C}$ 选择随机的 $M^* \in \{0,1\}^m$，计算 $CT^* = \text{DA-Encrypt}(M^*, ID_s^*, ID_r^*, sk_s^*)$，并将 CT^* 作为挑战密文发送给 $\mathcal{A}_1$。

问询阶段 2： 对于 $\mathcal{A}_1$ 的问询，$\mathcal{C}$ 的响应与问询阶段 1 相同。$\mathcal{A}_1$ 的约束如下:

(1) ID_s^* 和 ID_r^* 不可以被提交至私钥提取询问。

(2) CT^* 不可以被提交至可否认认证解密询问。

猜测阶段： $\mathcal{A}_1$ 输出 M'。若 $M' = M^*$，则在上述游戏中 $\mathcal{A}_1$ 获胜。$\mathcal{A}_1$ 获胜的优势可被定义为以下函数:

$$\text{Adv}_{\mathcal{A}_1}^{\text{OW-ID-CCA}} = \Pr[M' = M^*] \tag{2}$$

定义 1 (针对敌手 $\mathcal{A}_1$ 的 OW-ID-CCA) 如果对于任何多项式时间敌手 $\mathcal{A}_1$，在挑战者 $\mathcal{C}$ 的后续游戏中 $\mathcal{A}_1$ 的成功概率在安全参数 λ 条件下可忽略不计，则本方案对于敌手 $\mathcal{A}_1$ 是 OW-ID-CCA 安全的。

3.1.2 选择身份与密文攻击下的不可区分性(IND-ID-CCA)

本方案的 IND-ID-CCA 安全模型通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}_2$ 之间的安全游戏进行定义，该安全游戏描述如下:

第二类敌手 $\mathcal{A}_2$：第二类敌手没有接收方的陷门，该类型敌手的目的是区分挑战密文是由两个选定明文中的哪一个加密得到。

初始化： 挑战者 $\mathcal{C}$ 将安全参数 λ 作为输入，运行 Setup 算法生成系统参数 $Param$ 并将其传递给 $\mathcal{A}_2$，并生成主密钥 msk 由自己保管。

问询阶段 1： $\mathcal{A}_2$ 可以以任意顺序多次进行以下询问。

私钥提取询问：$\mathcal{A}_2$ 询问与身份 ID_u 相关的私钥，$\mathcal{C}$ 运行 ExtractKey 算法并返回对应的私钥 sk_u 给 $\mathcal{A}_2$。

可否认认证加密询问：$\mathcal{A}_2$ 选择明文 M，发送方身份 ID_s 与接收方身份 ID_r 提交给 $\mathcal{C}$。$\mathcal{C}$ 首先运行 ExtractKey 算法获得发送方的私钥 sk_s，再运行 DA-Encrypt 生成密文 CT，并将 CT 返回给 $\mathcal{A}_2$。

可否认认证解密询问：$\mathcal{A}_2$ 选择密文 CT 和接收方身份 ID_r 提交给 $\mathcal{C}$。$\mathcal{C}$ 首先运行 ExtractKey 获得接收方的私钥 sk_r，再运行 DA-Decrypt 生成明文 M。若 M 是有效密文，则返回给 $\mathcal{A}_2$，否则返回错误 $\perp$。

挑战阶段: $\mathcal{A}_2$ 结束问询阶段 1, 选择没有进行过私钥提取询问的发送方身份 ID_s^* 和接收方身份 ID_r^* 以及两个等长明文 $M_0, M_1 \in \{0,1\}^m$ 给挑战者 $\mathcal{C}$, $\mathcal{C}$ 选择一个随机比特 $\beta \in \{0,1\}$, 然后计算 $CT^* = \text{DA-Encrypt}(M_\beta^*, ID_s^*, ID_r^*, sk_s^*)$, 并将 CT^* 作为挑战密文发送给 $\mathcal{A}_2$。

问询阶段 2: 对于 $\mathcal{A}_2$ 的问询, $\mathcal{C}$ 的响应与问询阶段 1 相同。$\mathcal{A}_2$ 的约束如下:

(1) ID_s^* 和 ID_r^* 不可以被提交至私钥提取询问。

(2) CT^* 不可以被提交至可否认证解密询问。

猜测阶段: $\mathcal{A}_2$ 输出 $\beta' \in \{0,1\}$。若 $\beta' = \beta$, 则在上述游戏中 $\mathcal{A}_2$ 获胜。$\mathcal{A}_2$ 获胜的优势可被定义为以下函数:

$$\text{Adv}_{\mathcal{A}_2}^{\text{IND-ID-CCA}} = |\Pr[\beta' = \beta] - \frac{1}{2}| \tag{3}$$

定义 2 (针对敌手 $\mathcal{A}_2$ 的 IND-ID-CCA) 如果对于任何多项式时间敌手 $\mathcal{A}_2$, 在挑战者 $\mathcal{C}$ 的后续游戏中 $\mathcal{A}_2$ 的成功概率在安全参数 λ 中可忽略不计, 则本方案对于敌手 $\mathcal{A}_2$ 是 IND-ID-CCA 安全的。

3.1.3 选择身份与消息攻击下的可否认认证性 (DA-ID-CMA)

方案的 DA-ID-CMA 安全模型通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{F}$ 之间的安全游戏进行定义, 该安全游戏描述如下:

第三类敌手 $\mathcal{F}$: 第三类敌手没有发送方和接收方的私钥, 该类型敌手的目的是伪造出合法的密文。

初始化: 挑战者 $\mathcal{C}$ 将安全参数 λ 作为输入, 运行 Setup 算法生成系统参数 *Param* 并将其传递给 $\mathcal{F}$, 并生成主密钥 *msk* 由自己保管。

攻击阶段: 敌手 $\mathcal{F}$ 可以在多项式时间内发起类似于 IND-ID-CCA 游戏的询问。

伪造阶段: 游戏结束后, 敌手 $\mathcal{F}$ 生成伪造密文 CT', 并且在以下条件满足时获胜:

(1) 通过对伪造密文 CT' 进行解密, 生成的 $\text{DA-Decrypt}(CT', ID_s^*, ID_r^*, sk_r^*) = M'$ 是有效密文。

(2) $\mathcal{F}$ 没有提交 ID_s^* 和 ID_r^* 至私钥提取询问。

(3) 敌手 $\mathcal{F}$ 没有对消息 M^* 进行可否认认证加密的问询。

定义 3 (针对敌手 $\mathcal{F}$ 的 DA-ID-CMA) 如果对于任意的多项式时间敌手 $\mathcal{F}$, 其赢得该游戏的优势是可忽略的, 则本方案被认为对敌手 $\mathcal{F}$ 是 DA-ID-CMA 安全的。

3.2 IB-DAE-ET 具体构造

本章节给出了 IB-DAE-ET 方案的具体构造, 包括了以下六个算法。

Setup: 选取安全参数 λ, 阶数为素数 p 的两个群 G_1, G_2, 定义双线性映射 $e: G_1 \times G_1 \to G_2$。选取 g 作为群 G_1 的生成元。$\text{H}_1, \text{H}_2, \text{H}_3$ 是三个哈希函数, 分别满足 $\text{H}_1: \{0,1\}^* \to G_1$, $\text{H}_2: G_2 \to Z_p^*$, $\text{H}_3: G_1 \to Z_p^*$。随机选择 $(s_1, s_2) \in Z_p^*$ 作为主密钥 *msk*, 计算系统公钥 $g_1 = g^{s_1}, g_2 = g^{s_2}$。系统参数 *Param* 公开为 $\{G_1, G_2, e, g, g_1, g_2, \text{H}_1, \text{H}_2, \text{H}_3\}$, 主密钥 *msk* 则保密。

ExtractKey: 当接收到来自用户的身份信息 ID_u 时, 本算法生成 $sk_u = (sk_{u,1}, sk_{u,2})$ 作为对应身份的私钥。其中发送方的私钥对是 $sk_{s,1} = \text{H}_1(ID_s)^{s_1}$, $sk_{s,2} = \text{H}_1(ID_s)^{s_2}$。接收方的私钥对是 $sk_{r,1} = \text{H}_1(ID_r)^{s_1}$, $sk_{r,2} = \text{H}_1(ID_r)^{s_2}$。

Trapdoor: 输入接收方身份信息 ID_r, 本算法输出陷门 $td_r = sk_{r,2}$。

DA-Encrypt: 给定明文信息 $M \in G_1$, 发送方的身份 ID_s, 接收方的身份 ID_r。加密算法运行如下:

(1) 随机选择 $x_1, x_2 \in Z_p^*$;

(2) 计算 $CT_1 = g^{x_1}, CT_2 = g^{x_2}$;

(3) 计算 $\omega_1 = e(g_1, \text{H}_1(ID_r))^{x_1}$,

$\omega_2 = e(g_2, \text{H}_1(ID_r))^{x_2}$;

(4) 计算 $CT_3 = (M \| x_1) \oplus \text{H}_2(\omega_1)$,

$CT_4 = g^{\text{H}_2(\omega_2)+M}$;

(5) 计算 $z = \text{H}_3(M \| \text{H}_1(ID_s) \| \text{H}_1(ID_r) \| CT_1)$;

(6) 计算 $CT_5 = e(sk_{s,1}^z, \text{H}_1(ID_r))$, 密文的形式为 $CT = (CT_1, CT_2, CT_3, CT_4, CT_5)$;

DA-Decrypt: 给定密文 CT, 发送方的身份 ID_s, 接收方的私钥对 $(sk_{r,1}, sk_{r,2})$, 解密算法运行如下:

(1) 计算 $\omega_1 = e(CT_1, sk_{r,1})$;

(2) 计算 $M \| x_1 = CT_3 \oplus \text{H}_2(\omega_1)$;

(3) 验证 $CT_1 = g^{x_1}$,

计算 $z = \text{H}_3(M \| \text{H}_1(ID_s) \| \text{H}_1(ID_r) \| CT_1)$;

(4) 验证 $CT_5 = e(\text{H}_1(ID)_s^z, sk_{r,1})$。当且仅当上述式子同时满足时接收明文 M, 否则返回错误 $\perp$。

Test: 对于参与等式测试的不同用户 i,j, 分别存在不同的密文 $CT_i=(CT_{i,1},CT_{i,2},CT_{i,3},CT_{i,4},CT_{i,5})$ 和 $CT_j=(CT_{j,1},CT_{j,2},CT_{j,3},CT_{j,4},CT_{j,5})$。等式测试算法运行如下:

如果 $CT_{i,4}\cdot g^{-\mathrm{H}_2(e(CT_{i,2},td_i))}=CT_{j,4}\cdot g^{-\mathrm{H}_2(e(CT_{j,2},td_j))}$, 则说明 CT_i 和 CT_j 由相同的明文加密得到, 此时返回 1, 否则返回 0。

可否认性: 在本方案中, 拥有 $sk_{r,1}$ 的接收方在解密后可以生成一种密文, 该密文与拥有 $sk_{s,1}$ 的发送方生成的密文在第三方处无法区分。模拟接收方对给定 M 生成可否认密文的过程如下:

(1) 随机选择 $\overline{x_1},\overline{x_2}\in Z_p^*$, 其取值个数为 $\phi(p)=p-1$;

(2) 计算 $\overline{CT_1}=g^{\overline{x_1}}$, $\overline{CT_2}=g^{\overline{x_2}}$;

(3) 计算 $\overline{\omega_1}=e(g_1,\mathrm{H}_1(ID_r))^{\overline{x_1}}$,

$\overline{\omega_2}=e(g_2,\mathrm{H}_1(ID_r))^{\overline{x_2}}$;

(4) 计算 $\overline{CT_3}=(M\,\|\,\overline{x_1})\oplus\mathrm{H}_2(\overline{\omega_1})$,

$\overline{CT_4}=g^{\mathrm{H}_2(\overline{\omega_2})+M}$;

(5) 计算 $\overline{z}=\mathrm{H}_3(M\,\|\,\mathrm{H}_1(ID_s)\,\|\,\mathrm{H}_1(ID_r)\,\|\,\overline{CT_1})$

(6) 计算 $\overline{CT_5}=e(\mathrm{H}_1(ID)_s^{\overline{z}},sk_{r,1})$。

由接收方生成的 $\overline{CT}=(\overline{CT_1},\overline{CT_2},\overline{CT_3},\overline{CT_4},\overline{CT_5})$ 与原始密文 CT 是无法区分的。设 $\widehat{CT}=(\widehat{CT_1},\widehat{CT_2},\widehat{CT_3},\widehat{CT_4},\widehat{CT_5})$ 是发送方有效密文集中的任意一个。因为 $\overline{CT}$ 是随机生成的, 可得 $Pr[\overline{CT}=\widehat{CT}]$ 的概率为 $\dfrac{1}{p-1}$。同理可得, $Pr[\overline{CT}=CT]$ 的概率也为 $\dfrac{1}{p-1}$, 原因在于接收方生成的有效密文与原始密文均是 Z_p^* 中的随机元素产生的, 其概率分布相同。

3.3 安全性分析

定理 1 在随机预言模型中, 我们假设有一个敌手 $\mathcal{A}_{\mathrm{I}}$, 它可以在 OW-ID-CCA 游戏中运行并问询至多 q_{h_1} 次 H_1 问询, q_{h_2} 次 H_2 问询, q_{h_3} 次 H_3 问询, q_e 次可否认认证加密问询, q_d 次可否认认证解密问询, q_{key} 次私钥提取问询, q_{td} 次陷门问询, 最终在运行时间 t 内以 $\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}^{\text{OW-ID-CCA}}$ 的优势恢复目标密文。当有 q 个具体用户时, 存在一个算法 $\mathcal{C}$ 可以在运行时间 t' 最终以 $\mathrm{Adv}_{\mathcal{C}}^{\mathrm{BDH}}$ 解决 BDH 困难问题。其中:

$$\mathrm{Adv}_{\mathcal{C}}^{\mathrm{BDH}}\geqslant\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}^{\text{OW-ID-CCA}}-\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+q_{key}}{2^{lq(\lambda)}}\tag{4}$$

运行时间 $t'=\mathcal{O}(t+t_{h_1}+t_{h_2}+t_{h_3}+t_e+t_d+t_{td})$, $q_{ddh}=\mathcal{O}(q_{h_1}+q_{h_2}+q_{h_3}+q_d)$。这里的 $t_{h_1},t_{h_2},t_{h_3},t_e,t_d,t_{key},t_{td}$ 表示 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$ 三个随机预言机, 以及可否认认证加密, 可否认认证解密, 私钥提取和陷门问询的模拟时间。

证明: $\mathcal{C}$ 收到了一个 BDH 问题的随机元组 (g,g^a,g^b,g^c) 并尝试计算出 g^{abc}。证明的核心思想是 $\mathcal{C}$ 将 $\mathcal{A}_{\mathrm{I}}$ 作为子程序, 并在 OW-ID-CCA 游戏中作为 $\mathcal{A}_{\mathrm{I}}$ 的挑战者。$\mathcal{A}_{\mathrm{I}}$ 可以向 $\mathcal{C}$ 提出加密, 解密, 私钥提取和陷门问询。除此之外, $\mathcal{A}_{\mathrm{I}}$ 还可以向 $\mathcal{C}$ 问询随机预言机 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$。

初始化: $\mathcal{C}$ 运行 Setup 生成公共参数 *Param* 和 *msk*, $\mathcal{C}$ 将 *Param* 发送给 $\mathcal{A}_{\mathrm{I}}$, *msk* 则由自己保管。然后 $\mathcal{C}$ 选取随机的 α,β, 设定 $g_1=g^{\alpha a}$, $g_2=g^{\beta a}$。同时设置表 $L_k,L_{H_1},L_{H_2},L_{H_3}$ 用于应答 $\mathcal{A}_{\mathrm{I}}$ 的询问。

问询阶段 1: $\mathcal{C}$ 按如下方式应答 $\mathcal{A}_{\mathrm{I}}$ 的询问。

H_1 问询: 本游戏中, 一旦收到基于身份 ID_u 的请求, $\mathcal{C}$ 首先查找表 L_{H_1} 中有无对应的值。若有, 则直接返回对应 R_u。若没有, 则选取随机的 $\gamma\in Z_p^*$, 然后进行判定。设定一个 $\theta\in\{0,1\}$, 当 $\theta=0$ 时, $\mathcal{C}$ 返回 $R_u=g^{\gamma}$; 当 $\theta=1$ 时, $\mathcal{C}$ 返回 $R_u=g^{\gamma b}$。然后将对应的 (ID_u,γ,R_u,θ) 存入 L_{H_1} 中。

H_2 问询: 当 $\mathcal{A}_{\mathrm{I}}$ 询问 δ 时, $\mathcal{C}$ 随机选取 $h_2\in Z_p^*$ 作为返回值返回给 $\mathcal{A}_{\mathrm{I}}$, 并将 (δ,h_2) 存入 L_{H_2} 中。

H_3 问询: 当 $\mathcal{A}_{\mathrm{I}}$ 询问 η 时, $\mathcal{C}$ 随机选取 $h_3\in Z_p^*$ 作为返回值返回给 $\mathcal{A}_{\mathrm{I}}$, 并将 (η,h_3) 存入 L_{H_3} 中。

私钥提取问询: $\mathcal{A}_{\mathrm{I}}$ 选中某个接收方 ID_u 并询问其私钥, $\mathcal{C}$ 做如下判断:

(1)当 $\theta=1$ 时, $\mathcal{C}$ 拒绝询问请求, 游戏结束。

(2) 当 $\theta=0$ 时, $\mathcal{C}$ 运行 ExtractKey 算法生成 $sk_u=(sk_{u,1},sk_{u,2})$ 发送给 $\mathcal{A}_{\mathrm{I}}$, 并在 L_k 中记录下 (ID_u,sk_u)。

陷门问询: $\mathcal{A}_{\mathrm{I}}$ 输入某个接收方的 ID_r, $\mathcal{C}$ 做如下判断:

(1) 当 $\theta=0$ 时, $\mathcal{C}$ 查找表 L_k, 如果 ID_r 的表项 (ID_u, sk_u) 存在则直接返回 $td_r=sk_{r,2}$, 否则运行 ExtractKey 生成 $td_r=sk_{r,2}$ 并发送给 $\mathcal{A}_1$。

(2) 当 $\theta=1$ 时, $\mathcal{C}$ 计算 $td_r=g^{\gamma b}$ 并发送给 $\mathcal{A}_1$。

可否认认证加密问询: 当 $\mathcal{A}_1$ 选择发送方 ID_s, 接收方 ID_r 作为目标, 对明文 M 进行可否认加密询问时, $\mathcal{C}$ 首先进行判断:

(1) 当 $\theta=0$ 时, 则 $\mathcal{C}$ 正常运行 ExtractKey 和 DA-Encrypt 算法, 生成密文 $CT=(CT_1, CT_2, CT_3, CT_4, CT_5)$ 返回给 $\mathcal{A}_1$。

(2) 当 $\theta=1$ 时, 选择 $x_1, x_2 \in Z_p^*$, 并计算 $\delta=e(g_1, \mathrm{H}_1(ID_r))^{x_1}$, $\eta=e(g_2, \mathrm{H}_1(ID_r))^{x_2}$。然后 $\mathcal{C}$ 问询 H_2, H_3 得到返回值, 并将 (δ, h_2), (η, h_3) 存入 L_{H_2} 和 L_{H_3} 中, 随机选择 $CT_5 \in G_2$,

计算: $CT_1=g^{x_1}$, $CT_2=g^{x_2}$, $CT_3=(M \| x_1) \oplus \delta$, $CT_4=g^{\eta+M}$。

返回 $CT=(CT_1, CT_2, CT_3, CT_4, CT_5)$ 给 $\mathcal{A}_1$。

可否认认证解密问询: 当 $\mathcal{A}_1$ 选择选择发送方 ID_s, 接收方 ID_r 作为目标, 对密文 $CT=(CT_1, CT_2, CT_3, CT_4, CT_5)$ 进行可否认认证解密问询时, $\mathcal{C}$ 做如下判断:

(1) 当 $\theta=0$ 时, 则 $\mathcal{C}$ 正常运行 DA-Decrypt 算法, 返回明文 M 并进行检验, 检验合法则返回给 $\mathcal{A}_1$, 否则终止解密。

(2) 当 $\theta=1$ 时, 则 $\mathcal{C}$ 中止解密。

挑战阶段: $\mathcal{A}_1$ 结束问询阶段, 选中选择发送方 ID_s, 接收方 ID_s 作为目标发起挑战。挑战者 $\mathcal{C}$ 作如下判断:

(1)当 $\theta=0$ 时, $\mathcal{C}$ 中止挑战。

(2) 当 $\theta=1$ 时, 则 $\mathcal{C}$ 随机选择 $M^* \in \{0,1\}^m$, $x_2^* \in Z_p^*$, 计算 $CT^*=(CT_1^*, CT_2^*, CT_3^*, CT_4^*, CT_5^*)$ 并返回给 $\mathcal{A}_1$, 具体是:

$CT_1^*=g^{\epsilon c}$, $CT_2^*=g^{x_2^*}$, $CT_3^* \in_R G_1$,

$CT_4^*=g^{\mathrm{H}_2(\eta^*)+M^*}$, $CT_5^* \in_R G_2$。

问询阶段 2: $\mathcal{A}_1$ 继续进行类似于问询阶段 1 的问询, 除了以下限制:

(1) 目标用户 ID_s^*, ID_r^* 不可以被提交至私钥问询。

(2) CT^* 不可以被提交至可否认认证解密询问。

猜测阶段: 模拟完成后, $\mathcal{A}_1$ 输出 M'。然后 $\mathcal{C}$ 可以从 L_{H_2} 中随机选择 (δ^*, h_2^*), 计算出 $\delta^{*(\alpha\gamma\epsilon)^{-1}}=e(g,g)^{abc}$ 作为 BDH 问题的解。

接下来分析 $\mathcal{C}$ 成功的概率, 记 $\mathcal{A}_1$ 询问到 $\mathrm{H}_2(\omega_l^*)$ 为事件 E_1; 由于 $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ 碰撞而导致 $\mathcal{C}$ 终止加密询问为事件 E_2; $\mathcal{C}$ 拒绝有效加密密文为事件 E_3; $\mathcal{A}_1$ 在私钥问询中询问到 ID_s^*, ID_r^* 为事件 E_4。

$$\Pr[M'=M^*] \geqslant \Pr[E_1]=\frac{1}{2^{lq(\lambda)}}$$

$$\mathrm{Adv}_{\mathcal{A}_1}^{\text{OW-ID-CCA}} \geqslant \Pr[E_1]=\frac{1}{2^{lq(\lambda)}};$$

$$\Pr[E_2] \leqslant \frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})}{2^{lq(\lambda)}};$$

$$\Pr[E_3] \leqslant \frac{q_d}{2^{lq(\lambda)}};$$

$$\Pr[E_4] \leqslant \frac{q_{key}}{2^{lq(\lambda)}};$$

综上所述, 在 OW-ID-CCA 游戏中, 敌手 $\mathcal{A}_1$ 的优势为:

$$\mathrm{Adv}_{\mathcal{C}}^{\text{BDH}}+\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+q_{key}}{2^{lq(\lambda)}} \quad (5)$$

定理 2 在随机预言模型中, 我们假设有一个敌手 $\mathcal{A}_2$, 它可以在 IND-ID-CCA 游戏中运行并问询至多 q_{h_1} 次 H_1 问询, q_{h_2} 次 H_2 问询, q_{h_3} 次 H_3 问询, q_e 次可否认认证加密问询, q_d 次可否认认证解密问询, q_{key} 次私钥提取问询, 最终在运行时间 t 内以 $Adv_{\mathcal{A}_2}^{\text{IND-ID-CCA}}$ 的优势恢复目标密文。当有 q 个具体用户时, 存在一个算法 $\mathcal{C}$ 可以在运行时间 t' 最终以 $Adv_{\mathcal{C}}^{\text{BDH}}$ 解决 BDH 困难问题。其中,

$$\mathrm{Adv}_{\mathcal{C}}^{\text{BDH}} \geqslant \mathrm{Adv}_{\mathcal{A}_2}^{\text{IND-ID-CCA}} - \frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+q_{key}}{2^{lq(\lambda)}} \quad (6)$$

运行时间 $t'=\mathcal{O}(t+t_{h_1}+t_{h_2}+t_{h_3}+t_e+t_d)$, $q_{ddh}=\mathcal{O}(q_{h_1}+q_{h_2}+q_{h_3}+q_d)$。这里的 $t_{h_1}, t_{h_2}, t_{h_3}, t_e, t_d, t_{key}$ 表示 $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ 三个随机预言机, 以及可否认认证加密, 可否认认证解密和私钥提取问询的模拟时间。

证明: $\mathcal{C}$ 收到了一个 BDH 问题的随机元组 (g, g^a, g^b, g^c) 并尝试计算出 g^{abc}。证明的核心思想是 $\mathcal{C}$ 将 $\mathcal{A}_2$ 作为子程序, 并在 IND-ID-CCA 游戏中作为 $\mathcal{A}_2$ 的挑战者。$\mathcal{A}_2$ 可以向 $\mathcal{C}$ 提出加密, 解密和私钥提取问询。除此之外, $\mathcal{A}_2$ 还可以向 $\mathcal{C}$ 问询随机预言

机 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$。

初始化: $\mathcal{C}$ 运行 Setup 生成公共参数 *Param* 和 *msk*, $\mathcal{C}$ 将 *Param* 发送给 $\mathcal{A}_2$, *msk* 则由自己保管。然后 $\mathcal{C}$ 选取随机的 α,β, 设定 $g_1=g^{\alpha a}$, $g_2=g^{\beta a}$。同时设置表 $L_k,L_{H_1},L_{H_2},L_{H_3}$ 用于应答 $\mathcal{A}_2$ 的询问。

问询阶段 1: $\mathcal{C}$ 按如下方式应答 $\mathcal{A}_2$ 的询问。

H_1 问询: 本游戏中, 一旦收到基于身份 ID_u 的请求, $\mathcal{C}$ 首先查找表 L_{H_1} 中有无对应的值。若有, 则直接返回对应 R_u。若没有, 则选取随机的 $\gamma\in Z_p^*$, 然后进行判定。设定一个 $\theta\in\{0,1\}$, 当 $\theta=0$ 时, $\mathcal{C}$ 返回 $R_u=g^{\gamma}$; 当 $\theta=1$ 时, $\mathcal{C}$ 返回 $R_u=g^{\gamma b}$。然后将对应的 (ID_u,γ,R_u,θ) 存入 L_{H_1} 中。

H_2 问询: 当 $\mathcal{A}_2$ 询问 δ 时, $\mathcal{C}$ 随机选取 $h_2\in Z_p^*$ 作为返回值返回给 $\mathcal{A}_2$, 并将 (δ,h_2) 存入 L_{H_2} 中。

H_3 问询: 当 $\mathcal{A}_2$ 询问 η 时, $\mathcal{C}$ 随机选取 $h_3\in Z_p^*$ 作为返回值返回给 $\mathcal{A}_2$, 并将 (η,h_3) 存入 L_{H_3} 中。

私钥提取问询: $\mathcal{A}_2$ 选中某个接收方 ID_u 并询问其私钥, $\mathcal{C}$ 做如下判断:

(1) 当 $\theta=0$ 时, $\mathcal{C}$ 运行 ExtractKey 生成 $sk_u=(sk_{u,1},sk_{u,2})$ 发送给 $\mathcal{A}_2$, 并在 L_k 中记录下 (ID_u,sk_u)。

(2) 当 $\theta=1$ 时, $\mathcal{C}$ 拒绝询问请求, 游戏结束。

可否认认证加密问询: 当 $\mathcal{A}_2$ 选择发送方 ID_s, 接收方 ID_r 作为目标, 对明文 M 进行可否认加密询问时, $\mathcal{C}$ 首先进行判断:

(1) 当 $\theta=0$ 时, 则 $\mathcal{C}$ 正常运行 ExtractKey 和 DA-Encrypt 算法, 生成密文 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$ 返回给 $\mathcal{A}_2$。

(2) 当 $\theta=1$ 时, 选择 $x_1,x_2\in Z_p^*$, 并计算 $\delta=e(g_1,\mathrm{H}_1(ID_r))^{x_1}$, $\eta=e(g_2,\mathrm{H}_1(ID_r))^{x_2}$。然后 $\mathcal{C}$ 问询 H_2, H_3 得到返回值, 并将 (δ,h_2), (η,h_3) 存入 L_{H_2} 和 L_{H_3} 中, 随机选择 $CT_5\in G_2$,

计算: $CT_1=g^{x_1}$, $CT_2=g^{x_2}$, $CT_3=(M\,\|\,x_1)\oplus\delta$, $CT_4=g^{\eta+M}$。

返回 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$ 给 $\mathcal{A}_2$。

可否认认证解密问询: 当 $\mathcal{A}_2$ 选择选择发送方 ID_s, 接收方 ID_r 作为目标, 对密文 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$ 进行可否认认证解密问询时, $\mathcal{C}$ 做如下判断:

(1) 当 $\theta=0$ 时, 则 $\mathcal{C}$ 正常运行 DA-Decrypt 算法, 返回明文 M 并进行检验, 检验合法则返回给 $\mathcal{A}_2$, 否则终止解密。

(2) 当 $\theta=1$ 时, 则 $\mathcal{C}$ 中止解密。

挑战阶段: $\mathcal{A}_2$ 结束问询阶段, 选中选择发送方 ID_s, 接收方 ID_r 并发送两条等长的明文 $M_0,M_1\in G_1$ 给挑战者 $\mathcal{C}$。挑战者 $\mathcal{C}$ 作如下判断:

(1) 当 $\theta=0$ 时, $\mathcal{C}$ 中止挑战。

(2) 当 $\theta=1$ 时, 则 $\mathcal{C}$ 随机选择 $\beta\in\{0,1\}$, $x_2^*\in Z_p^*$, 计算 $CT^*=(CT_1^*,CT_2^*,CT_3^*,CT_4^*,CT_5^*)$ 并返回给 $\mathcal{A}_2$, 具体是:

$$CT_1^*=g^{\epsilon c},\ CT_2^*=g^{x_2^*},\ CT_3^*\in_R G_1,$$

$$CT_4^*=g^{\mathrm{H}_2(\eta^*)+M_\beta^*},\ CT_5^*\in_R G_2。$$

问询阶段 2: $\mathcal{A}_2$ 继续进行类似于问询阶段 1 的问询, 除了以下限制:

(1) 目标用户 ID_s^*, ID_r^* 不可以被提交至私钥问询。

(2) CT^* 不可以被提交至可否认认证解密询问。

猜测阶段: 模拟完成后, $\mathcal{A}_2$ 输出 M'。然后 $\mathcal{C}$ 可以从 L_{H_2} 中随机选择 (δ^*,h_2^*), 计算出 $\delta^{*(\alpha\gamma\epsilon)^{-1}}=e(g,g)^{abc}$ 作为 BDH 问题的解。

接下来分析 $\mathcal{C}$ 成功的概率, 记 $\mathcal{A}_2$ 询问到 $\mathrm{H}_2(\omega_1^*)$ 为事件 E_1; 由于 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$ 碰撞而导致 $\mathcal{C}$ 终止加密询问为事件 E_2; $\mathcal{C}$ 拒绝有效加密密文为事件 E_3, $\mathcal{A}_2$ 在私钥问询中询问到 ID_s^*, ID_r^* 为事件 E_4。

$$\Pr[\beta'=\beta]\leqslant\Pr[\beta'=\beta\,|\,\overline{E_1}]\Pr[\overline{E_1}]+\Pr[E_1];$$

$$\Pr[E_1]\geqslant 2\Pr[\beta'=\beta]-1=\mathrm{Adv}_{\mathcal{A}_2}^{\text{IND-ID-CCA}};$$

$$\Pr[E_2]\leqslant\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})}{2^{lq(\lambda)}};$$

$$\Pr[E_3]\leqslant\frac{q_d}{2^{lq(\lambda)}};$$

$$\Pr[E_4]\leqslant\frac{q_{key}}{2^{lq(\lambda)}};$$

综上所述, 在 IND-ID-CCA 游戏中, 敌手 $\mathcal{A}_2$ 的优势最多为:

$$\mathrm{Adv}_{\mathcal{C}}^{\mathrm{BDH}}+\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+q_{key}}{2^{lq(\lambda)}}\tag{7}$$

定理 3 在随机预言模型中, 我们假设有一个敌手 $\mathcal{F}$, 它可以在 DA-ID-CMA 游戏中运行并问询至多 q_{h_1} 次 H_1 问询, q_{h_2} 次 H_2 问询, q_{h_3} 次 H_3 问询, q_e

次可否认认证加密问询, q_d 次可否认认证解密问询, q_{key} 次私钥提取问询, 最终在运行时间 t 内以 $\mathrm{Adv}_{\mathcal{F}}^{\text{DA-ID-CMA}}$ 的优势伪造密文。那么存在一个算法 $\mathcal{C}$ 可以在运行时间 t' 内最终以 $Adv_{\mathcal{C}}^{\text{BDH}}$ 解决 BDH 困难问题。其中,

$$\mathrm{Adv}_{\mathcal{C}}^{\text{BDH}} \geqslant \mathrm{Adv}_{\mathcal{F}}^{\text{DA-ID-CMA}} - \frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+1}{2^{lq(\lambda)}} \tag{8}$$

运行时间 $t'=\mathcal{O}(t+t_{h_1}+t_{h_2}+t_{h_3}+t_e+t_d)$, $q_{ddh}=\mathcal{O}(q_{h_1}+q_{h_2}+q_{h_3}+q_d)$。这里的 $t_{h_1},t_{h_2},t_{h_3},t_e,t_d$ 表示 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$ 三个随机预言机, 以及可否认认证加密, 可否认认证解密和私钥提取问询的模拟时间。

证明: $\mathcal{C}$ 收到了一个 BDH 问题的随机元组 (g,g^a,g^b,g^c) 并尝试计算出 g^{abc}。证明的核心思想是 $\mathcal{C}$ 将 $\mathcal{F}$ 作为子程序, 并在 DA-ID-CMA 游戏中作为 $\mathcal{F}$ 的挑战者。$\mathcal{F}$ 可以向 $\mathcal{C}$ 提出可否认认证加密, 解密和私钥提取问询。除此之外, $\mathcal{F}$ 还可以向 $\mathcal{C}$ 问询随机预言机 $\mathrm{H}_1,\mathrm{H}_2,\mathrm{H}_3$。

初始化: $\mathcal{C}$ 运行 Setup 生成公共参数 *Param* 和 *msk*, $\mathcal{C}$ 将 *Param* 发送给 $\mathcal{F}$, *msk* 则由自己保管。然后 $\mathcal{C}$ 选取随机的 α,β, 设定 $g_1=g^{\alpha a}$, $g_2=g^{\beta a}$。同时设置表 L_{H_1},L_{H_2},L_{H_3} 用于应答 $\mathcal{F}$ 的询问。

攻击阶段: $\mathcal{C}$ 按如下方式应答 $\mathcal{F}$ 的询问。

H_1 问询: 本游戏中, $\mathcal{C}$ 设置两个标签 $i,j\in\{1,\ldots,q_{h_1}\}$ 分别对应发送方和接收方的身份。一旦收到基于身份 ID_u 的请求, $\mathcal{C}$ 进行如下判断:

(1) 若 $ID_u\neq ID_i,ID_j$, 则 $\mathcal{C}$ 设置 $R_u=\mathrm{H}_1(ID_u)=g^{\lambda}$, 并将 (ID_u,λ,R_u) 存入 L_{H_1} 中。

(2) 若 $ID_u=ID_i$, 则 $\mathcal{C}$ 设置 $R_u=\mathrm{H}_1(ID_u)=g^{\lambda b}$, 并将 (ID_u,λ,R_u) 存入 L_{H_1} 中。

(3) 若 $ID_u=ID_j$, 则 $\mathcal{C}$ 设置 $R_u=\mathrm{H}_1(ID_u)=g^{\gamma b}$, 并将 (ID_u,λ,R_u) 存入 L_{H_1} 中。

H_2 问询: 当 $\mathcal{F}$ 询问 δ 时, $\mathcal{C}$ 随机选取 $h_2\in\{0,1\}^*$ 作为返回值返回给 $\mathcal{F}$, 并将 (δ,h_2) 存入 L_{H_2} 中。

H_3 问询: 当 $\mathcal{F}$ 询问 η 时, $\mathcal{C}$ 随机选取 $h_3\in\{0,1\}^m$ 作为返回值返回给 $\mathcal{F}$, 并将 (η,h_3) 存入 L_{H_3} 中。

私钥提取问询: $\mathcal{F}$ 选中某个接收方 ID_u 并询问其私钥, $\mathcal{C}$ 做如下判断:

(1) 当 $ID_u=ID_i$ 或 $ID_u=ID_j$ 时, $\mathcal{C}$ 拒绝询问请求, 游戏结束。

(2) 当 $ID_u\neq ID_i,ID_j$ 时, $\mathcal{C}$ 运行 ExtractKey 生成 $sk_u=(sk_{u,1},sk_{u,2})$ 发送给 $\mathcal{F}$, 并在 L_k 中记录下 (ID_u,sk_u)。

可否认认证加密问询: 当 $\mathcal{F}$ 选择发送方 ID_s, 接收方 ID_r 作为目标, 对明文 M 进行可否认加密询问时, $\mathcal{C}$ 首先进行判断:

(1) 若 $ID_s\neq ID_i,ID_j,ID_r\neq ID_i,ID_j$, 则 $\mathcal{C}$ 运行 ExtractKey 算法和 DA-Encrypt 算法, 生成密文 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$ 返回给 $\mathcal{F}$。

(2) $ID_i\neq ID_s,ID_j=ID_r$ 或 $ID_i\neq ID_r,ID_j=ID_s$。$\mathcal{C}$ 首先运行 ExtractKey 算法得到 $sk_{i,1}\in G_1$, 再设置 $sk_{j,1}=g^{\lambda b}$, 将 $(\delta,*)$ 存入 L_{H_2} 中, 注意检查新生成的 δ 不可以与之前的 δ 重复。然后计算 $CT_1^*=g^{\epsilon c}$, $CT_2^*=g^{x_2^*}$, $CT_3^*\in_R G_1$, $CT_4^*=g^{\mathrm{H}_2(\eta^*)+M^*}$, $CT_5^*\in_R G_2$, 生成密文 $CT^*=(CT_1^*,CT_2^*,CT_3^*,CT_4^*,CT_5^*)$ 返回给 $\mathcal{F}$。

(3) 当 $ID_s=ID_i,ID_r=ID_j$ 时, $\mathcal{C}$ 首先选择 $sk_{i,1}=g^{\lambda b}$, $sk_{j,1}=g^{\gamma b}$, 将 $(\delta,*)$ 存入 L_{H_2} 中, 注意检查新生成的 δ 不可以与之前的 δ 重复。然后计算 $CT_1^*=g^{\epsilon c}$, $CT_2^*=g^{x_2^*}$, $CT_3^*\in_R G_1$, $CT_4^*=g^{\mathrm{H}_2(\eta^*)+M^*}$, $CT_5^*\in_R G_2$, 生成密文 $CT^*=(CT_1^*,CT_2^*,CT_3^*,CT_4^*,CT_5^*)$ 返回给 $\mathcal{F}$。

可否认认证解密问询: 当 $\mathcal{F}$ 选择选择发送方 ID_s, 接收方 ID_r 作为目标, 对密文 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$ 进行可否认认证解密问询时, $\mathcal{C}$ 做如下判断:

(1) 当 $ID_s\neq ID_i,ID_j,ID_r\neq ID_i,ID_j$ 时, 则 $\mathcal{C}$ 正常运行 DA-Decrypt 算法, 返回明文 M 并进行检验, 检验为合法明文则返回给 $\mathcal{F}$, 否则终止解密。

(2) 否则, $\mathcal{C}$ 中止解密。

伪造阶段: 在游戏的最后阶段, $\mathcal{F}$ 生成一个伪造的密文 $CT'=(CT_1,CT_2,CT_3',CT_4,CT_5')$。$\mathcal{C}$ 可以根据 CT' 生成同一组目标用户下加密的密文 $CT=(CT_1,CT_2,CT_3,CT_4,CT_5)$。

模拟完成后, $\mathcal{F}$ 输出 CT'。如果对应的 δ' 未在 L_{H_2} 中被询问到, 则 $\mathcal{C}$ 失败并终止游戏。否则, $\mathcal{C}$ 可

以借助 L_{H_2} 找出对应的 δ'，然后计算出 $\delta'^{(\alpha^{-1}\lambda^{-1}\epsilon^{-1})}=e(g,g)^{abc}$ 作为 BDH 问题的解。

接下来分析 $\mathcal{C}$ 成功的概率，记 $\mathcal{F}$ 在未询问 DA-Encrypt(M,ID_s^*,ID_r^*) 的情况下伪造出有效密文为事件 E_1；由于 H_1,H_2,H_3 碰撞而导致 $\mathcal{C}$ 终止加密询问为事件 E_2；$\mathcal{C}$ 拒绝有效加密密文为事件 E_3。

$$\Pr[E_1]\leqslant\frac{1}{2^{lq(\lambda)}};$$

$$\Pr[E_2]\leqslant\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})}{2^{lq(\lambda)}};$$

$$\Pr[E_3]\leqslant\frac{q_d}{2^{lq(\lambda)}};$$

综上所述，在DA-ID-CMA游戏中，敌手 $\mathcal{F}$ 的优势最多为:

$$\mathrm{Adv}_{\mathcal{C}}^{\mathrm{BDH}}+\frac{q_e(q_{h_1}+q_{h_2}+q_{h_3})+q_d+1}{2^{lq(\lambda)}} \tag{9}$$

4 理论及实验比较

在本节中，我们在表 1、2 和 3 中比较了本方案和一些相关工作[6,23,25,30]的计算开销、通讯开销和安全属性。为了保持一致性，我们定义 E 为一次配对运算，P 为一次双线性映射运算，$|Z_p|$表示群 Z_p 中一个元素的长度，$|G_1|$表示群 G_1 中一个元素的长度，$\{0,1\}^k$ 表示一个定长字符串的长度，T 表示时间戳,“√”表示实现了该功能,“×”表示不存在该功能。

从以上表格我们可以看出，最早被提出的等式测试方案[6]缺乏认证的功能，这导致任何人都可以执行等式测试。且该方案依赖的 W-IND-CCA2 安全模型是弱化版的 IND-CCA 安全模型，在遭受 CCA 类型攻击时并不适用。Ma 等人[30]的等式测试方案满足了可验证性，而且基于身份基进行构造。但是并不具有可否认认证功能，无法用于构造安全电子投票系统。Harn 等人[23]的方案证明了指定验证者签名的安全性。但指定验证者签名和加密的组合安全性还没有得到证明，而简单的组合会导致系统不安全，所以我们认为他们的方案没有提供完备的安全性证明。Li 等人[25]的方案将加密和可否认认证协议较好地结合，但是因为基于公钥加密系统，在证书管理方案有较大的开销。我们的方案可以同时满足可否认性和可验证性，且满足等式测试和可否认协议的安全模型要求，适用于电子投票系统。

为了评估上述方案的性能，我们实现了这些方案。本次实验平台的配置是 64 位 windows 操作系统，8GB 内存的 Intel®Core i7-7700 3.60GHz 处理器，Java 双线性对密码学库(Java pairing-based cryptography library, JPBC)[31]。JPBC 库是基于双线性对的公钥密码学的开发工具包，可以实现基于双线对的加解密算法方案。图 3~6 展示了相关方案不同维度的开销。

以上四幅图展示了相关工作[6, 23, 25, 30]和本方案的加密、解密、陷门生成(如果有)和等式测试(如果有)算法的时间开销。随着密文数量的增加，各方案的时间开销都有不同程度的增长。另外，由于方案[6,23,25]均基于公钥加密体制，在实际的应用环境不可避免地面临证书管理问题，这会迅速提升这

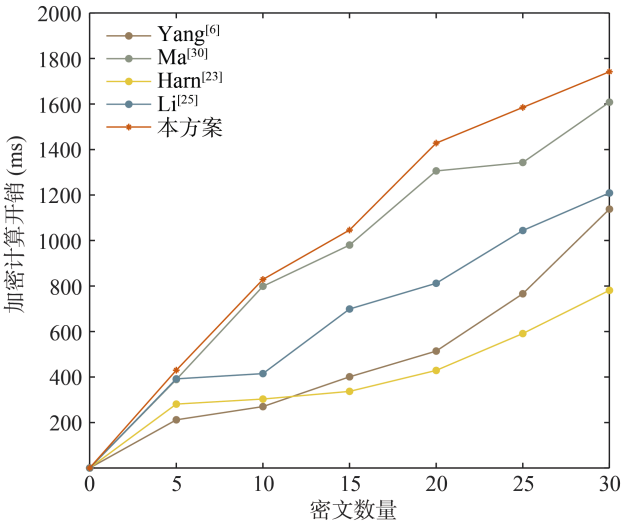


图 3 相关方案的加密开销模拟

Figure 3 Simulation of the encryption cost of related schemes

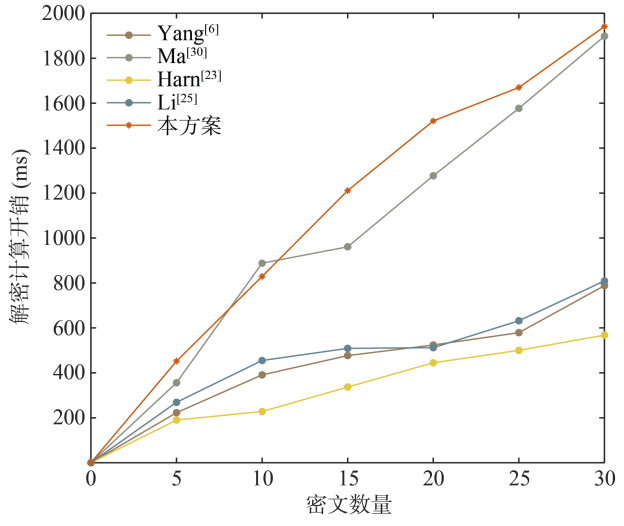


图 4 相关方案的解密开销模拟

Figure 4 Simulation of the decryption cost of related schemes

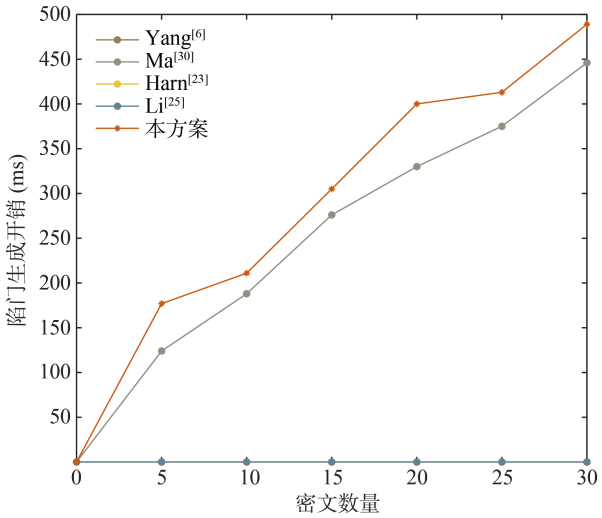


图 5　相关方案的陷门生成开销模拟

Figure 5　Simulation of the trapdoor generation cost of related schemes

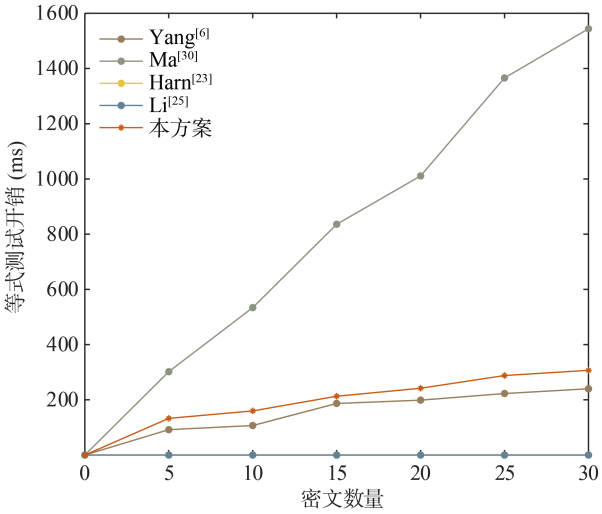


图 6　相关方案的等式测试开销模拟

Figure 6　Simulation of the equality test cost of related schemes

表 1　相关方案的计算开销对比

Table 1　Computation comparison of related schemes

方案	加密	解密	陷门	等式测试
Yang[6]	$3E$	$3E$	×	$2P$
Ma [30]	$6E+2P$	$2E+2P$	$2E$	$4P$
Harn[23]	$3E$	$4E$	×	×
Li[25]	$3E$	$3E$	×	×
本方案	$6E+3P$	$2E+2P$	$2E$	$2P$

些方案的时间开销。本方案较之其他方案首次将可否认加密与等式测试原语相结合，较为复杂的结构在时间开销上没有体现优势。但是作为回报，本方案同时实现了不可胁迫性和可审计性，拥有更丰富的功能。

表 2　相关方案的通讯开销对比

Table 2　Communication comparison of related schemes

方案	系统参数	私钥长度	陷门长度	密文长度
Yang[6]	$\|G_1\|$	$\|Z_p\|$	×	$2\|G_1\|+\{0,1\}^k$
Ma[30]	$2\|G_1\|$	$2\|Z_p\|$	$2\|G_1\|$	$4\|G_1\|+\{0,1\}^k$
Harn[23]	$2\|G_1\|$	$\|Z_p\|$	×	$2\|G_1\|+\{0,1\}^k+T$
Li[25]	$2\|G_1\|$	$2\|Z_p\|$	×	$3\|G_1\|+\{0,1\}^k$
本方案	$2\|G_1\|$	$2\|Z_p\|$	$\|G_1\|$	$4\|G_1\|+\{0,1\}^k$

表 3　相关方案的属性对比

Table 3　Properties of related schemes

方案	可认证	可否认性	形式化证明	身份基	安全性
Yang[6]	×	×	√	×	**W-IND-CCA2**
Ma[30]	√	×	√	√	**OW-ID-CCA**
Harn[23]	√	√	×	×	×
Li[25]	√	√	√	×	**IND-CCA**
本方案	√	√	√	√	**OW-ID-CCA** **IND-ID-CCA** **DA-ID-CMA**

5　一个安全的电子投票系统

本章我们使用提出的基于身份的支持等式测试的可否认加密方案设计了一个安全的电子投票系统，图 7 展示了该系统的结构。

选民自由指的是选民在选举中可以充分表达自身的诉求，在被不合理因素限制时也能选择自己心仪的候选人。选举的公平性指的是每张由选民选择的选票在选举后会被正确地统计，并受到有效的监督保护。在依照本方案设计的安全电子投票系统中，我们将目光聚焦到选民、计票者和审计机构上。首先选民会获得来自权威机构认证的身份信息，然后通过运行 DA-Encrypt(M, ID_s, ID_r, sk_s) 将投票内容 M 加密为选票 CT，并发送至计票者。该投票内容 M 实际上被可否认认证加密方法加密为选民可否认的选票 CT，在受到第三方胁迫时选民可以否认自己的投票结果，该系统从而达成了不可胁迫性。计票者运行 DA-Decrypt(C, ID_s, sk_r) 算法获得投票内容 M，从而验证选票的完整性，并将有效选票及用于运行等式测试的陷门 td_r 作为令牌发送给审计机构。审计机构在收到有效选票后，运行 Test(CT_i, CT_j) 算法。这里用于测试的密文是加密选票，本方案利用等式测试原语可在不解密选票的情况下来检验计票结果是否正确，进而对接收方的计票过程进行有效的审计，保护了安全投票系统的公平性。

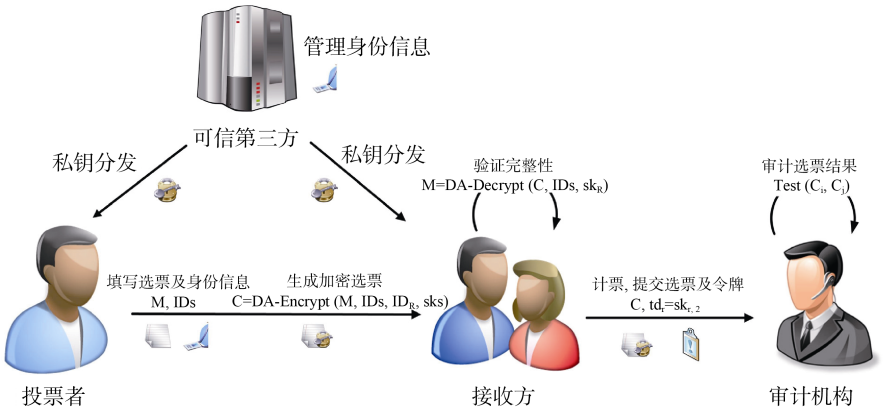


图 7　一个安全的电子投票系统

Figure 7　A secure e-voting system

6　总结

在本文中, 我们将可否认认证加密与等式测试技术相结合, 在身份基加密体制的基础上提出了支持等式测试的身份基可否认加密方案, 并在随机预言模型中证明其安全。本方案主要适用于电子投票系统, 满足了电子投票中需要的不可胁迫性和可审计性。我们还设计了一个应用本方案的安全电子投票系统。

在未来的研究中, 我们会针对异构系统来设计支持等式测试的可否认加密方案, 设计出更加适用于复杂网络环境中的安全电子投票系统, 并考虑使用更高效的安全假设优化算法结构, 进而提升系统的效率。

参考文献

[1] Buchsbaum T M. E-voting: International developments and lessons learnt[C]. *Electronic voting in Europe-Technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG. Gesellschaft für Informatik eV*, 2004.

[2] Lauer T W. The risk of e-voting[J]. *Electronic Journal of E-government*, 2004, 2(3): 177-186.

[3] Gritzalis D A. Principles and Requirements for a Secure E-Voting System[J]. *Computers & Security*, 2002, 21(6): 539-556.

[4] Moynihan D P. Building Secure Elections: E-Voting, Security, and Systems Theory[J]. *Public Administration Review*, 2004, 64(5): 515-528.

[5] Dwork C, Sahai A. Concurrent Zero-Knowledge: Reducing the Need for Timing Constraints[M]. Advances in Cryptology — CRYPTO '98. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 442-457.

[6] Yang, Guomin, Tan C H, Huang Qiong, et al. Probabilistic public key encryption with equality test[C]. *Cryptographers' track at the RSA conference*, 2010:119-131.

[7] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]. *2000 IEEE Symposium on Security and Privacy*, 2002: 44-55.

[8] Boneh D, Giovanni D C, Rafail O, et al. Public key encryption with keyword search[C]. *International conference on the theory and applications of cryptographic techniques*, 2004: 506-522.

[9] Tang Qiang. Towards public key encryption scheme supporting equality test with fine-grained authorization[C]. *Australasian conference on information security and privacy*, 2011: 389-406.

[10] Ma S, Huang Q, Zhang M W, et al. Efficient Public Key Encryption with Equality Test Supporting Flexible Authorization[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(3): 458-470.

[11] Xu Y, Wang M, Zhong H, et al. Verifiable Public Key Encryption Scheme with Equality Test in 5G Networks[J]. *IEEE Access*, 2017, 5: 12702-12713.

[12] Huang K B, Tso R, Chen Y C. Somewhat Semantic Secure Public Key Encryption with Filtered-Equality-Test in the Standard Model and Its Extension to Searchable Encryption[J]. *Journal of Computer and System Sciences*, 2017, 89: 400-409.

[13] Qu H P, Yan Z, Lin X J, et al. Certificateless Public Key Encryption with Equality Test[J]. *Information Sciences*, 2018, 462: 76-92.

[14] Deng X, Zhu H, Lee C H. Deniable Authentication Protocols[J]. *IEE Proceedings - Computers and Digital Techniques*, 2001, 148(2): 101-104.

[15] Fan L, Xu C X, Li J H. Deniable Authentication Protocol Based on Deffie-Hellman Algorithm[J]. *Electronics Letters*, 2002, 38(14): 705.

[16] Diffie W, Hellman M. New Directions in Cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654.

[17] Yoon E J, Ryu E K, Yoo K Y. Improvement of Fan et al.'s Deniable Authentication Protocol Based on Diffie-Hellman Algorithm[J]. *Applied Mathematics and Computation*, 2005, 167(1): 274-280.

[18] Shao Z H. Efficient Deniable Authentication Protocol Based on Generalized ElGamal Signature Scheme[J]. *Computer Standards & Interfaces*, 2004, 26(5): 449-454.

[19] Harn L, Xu Y. Design of Generalised ElGamal Type Digital Signature Schemes Based on Discrete Logarithm[J]. *Electronics Letters*, 1994, 30(24): 2025-2026.

[20] Lu R X, Cao Z F. Non-Interactive Deniable Authentication Protocol Based on Factoring[J]. *Computer Standards & Interfaces*, 2005,

27(4): 401-405.

[21] Wang Y J, Li J H, Tie L. A Simple Protocol for Deniable Authentication Based on ElGamal Cryptography[J]. *Networks*, 2005, 45(4): 193-194.

[22] Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[J]. *IEEE Transactions on Information Theory*, 1985, 31(4): 469-472.

[23] Harn L, Ren J. Design of Fully Deniable Authentication Service for E-Mail Applications[J]. *IEEE Communications Letters*, 2008, 12(3): 219-221.

[24] Wang B, Song Z X. A Non-Interactive Deniable Authentication Scheme Based on Designated Verifier Proofs[J]. *Information Sciences*, 2009, 179(6): 858-865.

[25] Li F G, Zhong D, Takagi T. Efficient Deniably Authenticated Encryption and Its Application to E-Mail[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(11): 2477-2486.

[26] Jin C H, Chen G H, Yu C H, et al. Heterogeneous Deniable Authentication and Its Application to E-Voting Systems[J]. *Journal of Information Security and Applications*, 2019, 47: 104-111.

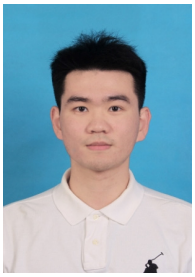
[27] Shamir A. Identity-Based Cryptosystems and Signature Schemes[M]. Advances in Cryptology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 47-53.

[28] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[M]. Advances in Cryptology — CRYPTO 2001. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 213-229.

[29] Abdalla M, Bellare M, Catalano D, et al. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions[M]. Advances in Cryptology – CRYPTO 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 205-222.

[30] Ma S. Identity-Based Encryption with Outsourced Equality Test in Cloud Computing[J]. *Information Sciences*, 2016, 328: 389-402.

[31] De Caro A, Iovino V. JPBC: Java Pairing Based Cryptography[C]. *2011 IEEE Symposium on Computers and Communications*, 2011: 850-855.



姚天昂 于 2022 年在电子科技大学软件工程专业获得硕士学位。现于南京大学计算机科学与技术系攻读博士学位。研究领域和兴趣为网络空间安全、公钥密码学、区块链。Email: tianangyao@gmail.com

熊虎 于 2009 年在电子科技大学信息与通信工程专业获得博士学位。现任电子科技大学信息与软件工程学院教授。研究领域和兴趣为网络空间安全、密码学。Email: xionghu.uestc@gmail.com