

具有密文等值测试功能的公钥加密技术综述

王元昊, 李宏博, 崔钰钊, 郭庆文, 黄琼

(华南农业大学数学与信息学院, 广东 广州 510642)

摘要: 作为解决云环境中多公钥加密计算问题的重要方法之一, 密文等值测试技术可以实现对不同公钥加密的数据进行比较, 使测试者在不对密文进行解密的前提下判断密文对应的明文是否相同。首先介绍了密文等值测试概念及其安全模型, 总结了目前提出的 6 种授权模式所适用的场景以及对应的输入与输出; 然后对比了密文等值测试技术与公钥可搜索加密技术的异同, 阐述并分析了包括公钥、基于身份和基于属性在内的若干典型密文等值测试方案; 最后讨论了密文等值测试的应用场景并对未来的研究进行展望。

关键词: 等值测试; 基于身份加密; 可搜索加密; 云计算

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018094

Survey on public key encryption with equality test

WANG Yuanhao, LI Hongbo, CUI Yuzhao, GUO Qingwen, HUANG Qiong

College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China

Abstract: As one of the important methods of solving the problem of computation over encrypted data under multiple public keys in cloud environment, public key encryption with equality test (PKEET) supports to check whether two ciphertexts encrypted under (possibly) different public keys contain the same message without decrypting the ciphertexts. Definitions, security models and six types of authorization modes of PKEET are introduced and summarized. Besides, the relationship between PKEET and public key encryption with keyword search (PKES) is discussed. Several typical public-key, identity-based and attribute-based encryption with equality test schemes proposed recently are analyzed and compared. Furthermore, some application scenarios and research directions are discussed.

Key words: equality test, identity-based encryption, searchable encryption, cloud computing

1 引言

随着信息技术的飞速发展, 云计算技术从实验室普及到了社会大众。云存储是云计算的一项主要服务, 它能方便地对数据进行备份与分享,

并能有效降低用户的存储成本, 带来便捷。近年来, 国内外也涌现了 Amazon、Dropbox、百度、360 等云存储服务供应商。

云计算的发展使用户对数据安全性越来越重视。企业用户在使用云存储时, 很有可能上传敏

收稿日期: 2018-10-10; 修回日期: 2018-10-30

通信作者: 黄琼, qhuang@scau.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61872152); 广东省自然科学基金杰出青年基金资助项目 (No.2014A030306021); 广东省特支计划基金资助项目 (No.2015TQ01X796); 广州市珠江科技新星专项基金资助项目 (No.201610010037)

Foundation Items: The National Natural Science Foundation of China (No.61872152), Guangdong Natural Science Funds for Distinguished Young Scholar (No.2014A030306021), Guangdong Program for Special Support of Top-notch Young Professionals (No.2015TQ01X796), Pearl River Nova Program of Guangzhou (No.201610010037)

感数据,如企业人事档案、患者医疗数据、环境监测数据等。然而,近年来数据泄露事故频发,用户可能会担心云存储服务供应商在用户不知情的情况下非法贩卖数据给第三方;再者,若遭到黑客入侵,以明文形式存储的数据将完全暴露给黑客。针对该问题,一种有效的办法是用户先将数据进行加密再上传数据,确保在不泄露密钥的情况下,任何人都无法在较短时间内解密数据,从而保护用户的隐私。然而,数据在加密后会失去原本的特点与结构,使在明文上的各种运算难以在密文上实施,导致原有的搜索算法不再奏效。

为了实现对加密数据搜索的需求,Boneh等^[1]提出了公钥可搜索加密(PEKS, public key encryption with keyword search),引起了研究人员的广泛兴趣,也为后继研究提供了指导。但该技术只能对使用了相同公钥加密的数据进行操作,考虑到云环境中用户可能会使用不同的公钥对数据进行加密,服务器不能直接对不同公钥加密的数据进行比较,使公钥可搜索加密技术存在一定的局限性。

因此,Yang等^[2]首次提出了密文等值测试公钥加密技术(PKEET, public key encryption with equality test)。该技术用于解决多公钥加密数据比较问题,即使加密时所使用的公钥不同,用户也可以在不进行解密的前提下,比较两段密文对应的明文是否相同。

密文等值测试技术有着广阔的应用场景,如过滤与归档电子邮件、根据标签对加密数据进行归类、实现数据库加密字段的连接操作等。传统方法难以对不同公钥加密的数据进行有效的归类,而使用密文等值测试技术则可以有效解决这个问题,具有重要研究意义和实用价值。

本文是对密文等值测试技术的研究进展进行归纳与总结,简述该技术的定义、安全模型与授权模式,并将部分典型的密文等值测试技术的方案进行分析与对比,最后对密文等值测试技术进行展望,期望能对国内的密文等值测试技术的研究起到推动作用。

2 密文等值测试技术介绍

公钥加密密文等值测试技术由Yang等^[2]在

CT-RSA 2010上首次提出,对公钥加密进行了拓展,增加了测试算法,可以对不同公钥加密的数据进行比较,受到广泛关注与研究。

密文等值测试技术中生成的密文通常可以分成两部分:一部分用于给接收者解密获取明文,而另一部分专门用于等值测试。基于双线性对的特性可以构造出特定的算法,使即使两份密文所使用的公钥不同,也可以进行判断两者所对应的明文是否相等。值得一提的是,密文等值测试是直接对密文进行比较,并不会对明文进行泄露,可以确保数据的保密性。具体流程如图1所示。

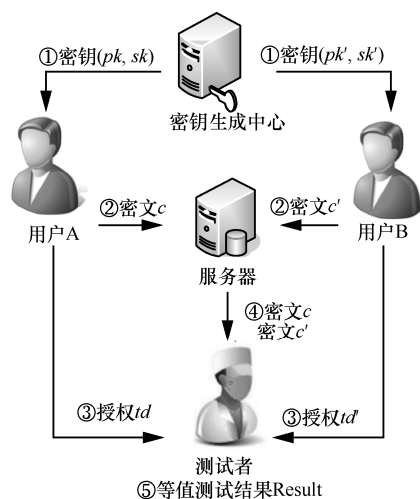


图1 密文等值测试流程

密文等值测试技术的提出在一定程度上解决了对多公钥加密数据计算的难题,丰富了云环境下公钥加密数据的检索方式,为公钥加密提出了新的研究方向。

2.1 方案描述

密文等值测试方案通常包含以下6个算法: $Setup$ 、 $KeyGen$ 、 Enc 、 Dec 、 Aut 、 $Test$, 而 $\mathbb{M}$ 与 $\mathbb{C}$ 分别是明文空间以及密文空间。其中

- 1) $Setup(\lambda) \rightarrow pp$: 初始化算法, 输入安全参数 λ , 输出系统参数 pp 。
- 2) $KeyGen(pp) \rightarrow (pk, sk)$: 密钥生成算法, 输入系统参数 pp , 输出公钥与私钥 (pk, sk) 。
- 3) $Enc(m, pk) \rightarrow c$: 加密算法, 输入待加密的明文 $m \in \mathbb{M}$ 与公钥 pk , 输出密文 c 。
- 4) $Dec(c, sk) \rightarrow m$: 解密算法, 输入待解密的密文 $c \in \mathbb{C}$ 与私钥 sk , 输出密文 m 。
- 5) $Aut(sk, \cdot) \rightarrow td$: 授权生成算法, 输入私

钥 sk 等, 输出授权 td 。

6) $Test(c, td, c', td') \rightarrow result$: 密文等值测试算法, 输入两组密文与对应的授权 (c, td) 与 (c', td') , 输出匹配结果: 若 c 与 c' 所对应的明文一样, 则输出 1; 否则输出 0。

此外, 对算法一致性进行了定义。

定义 1 (解密正确性): 对任意 $m \in \mathcal{M}$, $Dec(Enc(m, pk), sk) = m$ 。

定义 2 (测试一致性): 对任意 m 与 $m' \in \mathcal{M}$, 若 $m \in m'$, 且 $td = Aut(sk, \cdot)$, $td' = Aut(sk', \cdot)$, 则 $\Pr[Test(Enc(m, pk), td, Enc(m', pk'), td') = 1] = 1$ 。

定义 3 (测试可靠性): 对任意 m 与 $m' \in \mathcal{M}$, 若 $m \neq m'$, 且 $td = Aut(sk, \cdot)$, $td' = Aut(sk', \cdot)$, 则 $\Pr[Test(Enc(m, pk), td, Enc(m', pk'), td') = 1] \leq \text{negl}(\lambda)$ 。

2.2 安全模型

一个安全的密文等值测试方案应考虑如下 2 种类型的敌手。

1) Type-I 敌手: 在获取挑战密文所对应的陷门后, 试图猜出挑战密文所对应的明文。

2) Type-II 敌手: 没有获得挑战密文所对应的陷门, 但试图区分挑战密文对应哪个明文。

对于一个密文等值测试方案, 若敌手获得了挑战密文所对应的陷门, 显然敌手可以直接运行 Test 算法对挑战密文进行区分, 从而挑战成功。因此, 需要对敌手的能力进行限制。

对 Type-I 敌手的攻击, 定义了选择密文攻击下单向安全性 (OW-CCA, one-wayness under chosen ciphertext attacks); 对 Type-II 敌手的攻击, 定义了选择密文攻击下不可区分安全性 (IND-CCA, indistinguishability under chosen ciphertext attacks)。

为了方便形式化证明, 本文用以下游戏定义安全模型。

游戏 1 (OW-CCA 游戏): 令敌手 A_1 为 Type-I 敌手, 并预先设定好序号 $t(1 \leq t \leq k)$, 敌手 A_1 与挑战者 C 按如下步骤进行游戏。

① 始化阶段: 挑战者 C 运行 $Setup(\lambda)$ 得到系统参数 pp , 运行 $KeyGen(pp)$ 得到 k 对公钥与私钥 $(pk_i, sk_i)(1 \leq i \leq k)$, 并将 pp 与所有公钥 pk_i 发给敌手 A_1 。

② 询问阶段 1: 敌手 A_1 被允许在多项式时

间内对预言机进行下列 3 种询问。

私钥询问: 发送序号 i , 获取公钥 pk_i 对应的私钥 sk_i 。

解密询问: 发送序号 i 与密文 c_i , 获取密文 c_i 所对应的解密结果 $Dec(c_i, sk_i)$ 。

授权询问: 发送序号 i (有时也需要密文 c_i 或其他信息), 获取对应的陷门 td_i 。

其中, 敌手 A_1 不得在私钥询问时询问序号 t 获取私钥 sk_t 。

③ 挑战阶段: 挑战者 C 随机选择密文 $m \in \mathcal{M}$, 运行 $Enc(m, pk_t)$ 得到 c_t ; 挑战者 C 将 c_t 作为挑战密文发送给敌手 A_1 。

④ 询问阶段 2: 敌手 A_1 被允许在多项式时间内对预言机进行询问阶段 1 中的 3 种询问。其中, 敌手 A_1 不得在私钥询问时询问序号 t 获取私钥 sk_t , 且不得在解密询问时询问序号 t 与密文 c_t 获取所对应的解密结果。

⑤ 猜测阶段: 敌手 A_1 输出 $m' \in \mathcal{M}$ 。若 $m = m'$, 则敌手赢得游戏 1。

定义 4 若一个密文等值测试方案能够抵挡任意多项式时间 Type-I 敌手, 即

$$Adv_{A_1}^{\text{OW-CCA}}(\lambda) = \Pr[m = m'] \leq \text{negl}(\lambda)$$

则称该方案是 OW-CCA 安全的。

游戏 2 (IND-CCA 游戏): 令敌手 A_2 为 Type-II 敌手, 并预先设定好序号 $t(1 \leq t \leq k)$, 敌手 A_2 与挑战者 C 按如下步骤进行游戏:

① 初始化阶段: 挑战者 C 执行与游戏 1 的初始化阶段相同的操作。

② 询问阶段 1: 敌手 A_2 被允许在多项式时间内对预言机进行游戏 1 的询问阶段 1 中的 3 种询问, 并被加以相同的限制。

③ 挑战阶段: 敌手 A_2 选择两段相同长度的明文 $m_0, m_1 \in \mathcal{M}$ 发给挑战者 C; 挑战者 C 随机选择比特 $b \in \{0, 1\}$, 运行 $Enc(m_b, pk_t)$ 得到 c_t ; 挑战者 C 将 c_t 作为挑战密文发送给敌手 A_2 。

④ 询问阶段 2: 敌手 A_2 被允许在多项式时间内对预言机进行游戏 1 的询问阶段 2 中的 3 种询问, 并被加以相同的限制, 以及不得在授权询问时询问序号 t (与密文 c_t 等) 获取所对应的陷门。

⑤ 猜测阶段: 敌手 A_2 输出 $b' \in \{0, 1\}$ 。若 $b = b'$, 则敌手 A_2 赢得游戏 2。

定义 5 若一个密文等值测试方案能够抵挡任意多项式时间 Type-II 敌手, 即

$$Adv_{A_2}^{\text{IND-CCA}}(\lambda) = |\Pr[b = b'] - \frac{1}{2}| \leq \text{negl}(\lambda)$$

则称该方案是 IND-CCA 安全的。

2.3 密文等值测试与公钥可搜索加密的区别

密文等值测试技术可以看成是公钥可搜索加密的一种变体, 是公钥加密中一类新型密文搜索机制。两者均包含加密和陷门/授权生成算法, 可用于搜索关键字。PKEET 还可比较密文是否包含相同关键字, 而 PEKS 则不适合。

在云环境中, 由于用户数量众多, 单用户的公钥加密方案实用性不高。部分可搜索加密方案^[3-6]实现了多用户在密文上进行关键字检索的功能, 但由于机制限制, 只能对同一公钥所加密的密文进行检索, 多公钥的场景下则未能很好地处理。

文献[2]中提出可以将密文等值测试方案转化为公钥可搜索加密方案。在文献[7]的工作基础上, Huang 等^[8]则将标准模型下的密文等值测试方案拓展为公钥可搜索加密方案, 将密文等值测试技术与可搜索加密技术进行结合。

两者具体区别如表 1 所示。密文等值测试技

术支持对不同公钥加密的数据进行等值测试或关键字搜索, 但公钥可搜索加密技术只能处理单公钥加密的数据。

2.4 授权模式

Yang 等^[2]的密文等值测试方案中, 所有的输入都是公开的, 没有授权生成算法 (Aut), 使任何人都可进行等值测试。现实生活中的关键字数量有限, 这导致攻击者可能采取生成大量密文执行等值测试的方式来进行猜测攻击。因此, 许多学者^[9-13]对密文等值测试方案进行拓展, 提出了支持授权的密文等值测试方案, 要求测试者要得到授权才可进行等值测试。

Ma 等^[14]归纳了密文等值测试技术支持的 4 种类型的授权模式, 并提出了支持灵活授权的方案。Xu 等在文献[15]中提出了另外 2 种不同类型的授权模式。

如图 2 所示, 密文等值测试技术具体包含 6 种类型的授权模式。为了方便对授权模式进行说明, 设定如下场景: 假设 Alice、Bob、Cindy 等均为有特殊症状的病人, 每个人都持有多份使用各自公钥进行加密的病历。医疗机构希望在不泄露病人隐私的前提下查找有相同症状的病人, 则可根

表 1

密文等值测试技术与公钥可搜索加密比较

	对多公钥的支持	陷门生成	测试内容
密文等值测试技术	支持	与密文或加密者绑定	判断 2 个密文对应明文是否相等
公钥可搜索加密	不支持	与关键字绑定	判断密文是否包含特定关键字

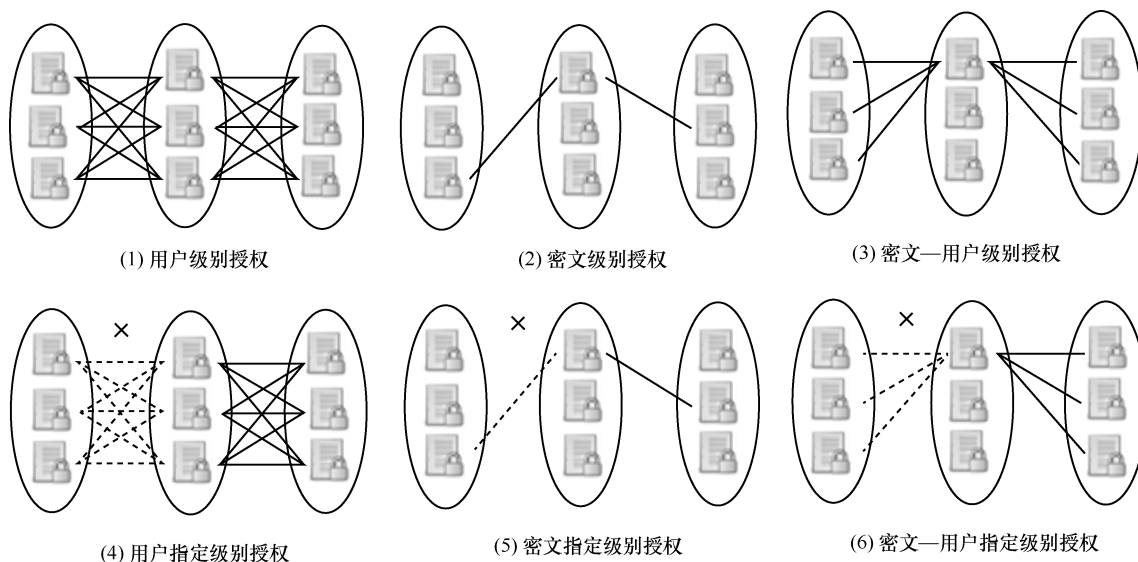


图 2 密文等值测试支持的 6 种授权模式

据病人所允许的授权类型级别进行病历匹配（即等值测试）。

1) 用户级别授权（多对多）

若 Alice 与其他病人都同意对所有历史病历进行病历匹配，则机构可以获取与本人绑定的陷门。Alice 与其他病人的陷门生成均需要各自的私钥 sk_i 。

在该授权模式，持有授权 $Aut_1(sk_{Alice})$ 与 $Aut_1(sk_{Bob})$ 的测试者可将 Alice 的任意密文与 Bob 的任意密文进行等值测试。

2) 密文级别授权（一对一）

若 Alice 与其他病人只同意对若干份病历进行病历匹配，则机构获取的陷门会与本人和具体的病历绑定，每个陷门对应一份病历。Alice 与其他病人的陷门生成均需要各自的私钥 sk_i 与病历密文 c_i 。

在该授权模式，持有授权 $Aut_2(sk_{Alice}, c_i)$ 与 $Aut_2(sk_{Bob}, c_j)$ 的测试者可将 Alice 的特定密文 c_i 与 Bob 的特定密文 c_j 进行等值测试。

3) 密文—用户级别授权（一对多）

该类型为 1) 和 2) 的结合。若 Alice 只同意对若干份病历进行病历匹配，而其他病人同意对所有历史病历进行病历匹配，Alice 的陷门生成需要私钥 sk_i 与病历密文 c_i ，其他病人的陷门生成需要私钥 sk_j 。

在该授权模式，持有授权 $Aut_{3,i}(sk_{Alice}, c_i)$ 与 $Aut_{3,j}(sk_{Bob})$ 的测试者可将 Alice 的特定密文 c_i 与 Bob 的任意密文进行等值测试。

4) 用户指定级别授权（指定多对多）

若 Alice 只希望自己的病历与指定的病人（如亲戚 Cindy）进行病历匹配，但同意对所有历史病历进行病历匹配，则机构获取的陷门会与本人以及指定的人绑定，每一对进行病历匹配的人需要一组陷门。Alice 与亲戚的陷门生成均需要各自的私钥 sk_i 与对方的公钥 sk_j 。

在该授权模式，只有持有 $Aut_4(sk_{Alice}, pk_{Cindy})$ 与 $Aut_4(sk_{Cindy}, pk_{Alice})$ 的测试者才可将 Alice 的任意密文与 Cindy 的任意密文进行等值测试。

5) 密文指定级别授权（指定一对一）

若 Alice 只希望自己的病历与指定的病人（如亲戚 Cindy）进行病历匹配，且只同意对若干份病历进行病历匹配，则每一对进行病历匹配的病

历都需要一组陷门。Alice 与亲戚的陷门生成均需要各自的私钥 sk_i 、病历密文 c_i 、对方的公钥 pk_j 与对方的密文 c_j 。

在该授权模式，只有持有授权 $Aut_5(sk_{Alice}, c_i, pk_{Cindy}, c_j)$ 与 $Aut_5(sk_{Cindy}, c_j, pk_{Alice}, c_i)$ 的测试者才可将 Alice 的特定密文 c_i 与 Cindy 的特定密文 c_j 进行等值测试。

6) 密文—用户指定级别授权（指定一对多）

该类型为(4)与(5)的结合。若 Alice 只希望自己的病历与指定的病人（如亲戚 Cindy）进行病历匹配，但 Alice 只同意对若干份病历进行病历匹配，而亲戚同意对所有历史病历进行病历匹配，则 Alice 的陷门生成需要私钥 sk_i 、病历密文 c_i 与对方的公钥 pk_j ，对方的陷门生成需要私钥 sk_j 与 Alice 的公钥 pk_i 。

在该授权模式，只有持有授权 $Aut_6(sk_{Alice}, c_i, pk_{Cindy})$ 与 $Aut_6(sk_{Cindy}, pk_{Alice})$ 的测试者才可将 Alice 的特定密文 c_i 与 Cindy 的任意密文进行等值测试。

在不同的授权模式下，授权生成算法的输入会略有不同，但生成的陷门 td 均为密文等值测试算法的输入。显然，获得相应的陷门，才可进行相应授权模式下的等值测试。

本文对若干典型密文等值测试方案进行了比较，其中包括指出各个方案所对应的授权模式。详细见第 4 节。

3 典型密文等值测试方案介绍

现有的密文等值测试方案针对用户密钥的管理方式可分为公钥加密的方案、基于身份的方案（IBEET 方案）与基于属性的方案（ABEET 方案）。此外，考虑到等值测试的现实使用场景，着重对支持授权与安全性提升进行研究。本节对若干典型密文等值测试方案进行介绍。

3.1 支持授权的密文等值测试方案

考虑到 Yang 等^[2]的方案存在未对等值测试进行授权的问题，任何人都可以对加密信息进行等值测试，存在一定的安全风险，Tang^[9]提出了支持细粒度授权的密文等值测试（FG-PKEET），使用户通过可信第三方进行等值测试的授权控制。该方案中，授权陷门由等值测试的双方共同协商后产生，只有持有该陷门才可以运行等值测

试算法。

随后, Tang 还提出了支持用户指定授权的密文等值测试 (AoN-PKEET)^[10] 与支持不同粒度授权的密文等值测试 (ADG-PKEET)^[11], 前者可以进行粗粒度控制, 授权陷门与用户绑定, 得到授权后可以对该用户的所有密文进行等值测试, 且等值测试只用到指数运算, 所设计的方案不需要双线性运算 (Pairing)。后者则是对 FG-PKEET 的拓展, 使用双代理抵抗离线消息恢复攻击 (offline message recovery attack), 但需要协议使双代理进行交互, 且计算开销较高。

Ma 等^[12]提出支持多用户授权的密文等值测试 (PKE-DET), 采取了委托第三方进行等值测试的方式, 授权陷门生成时需要用到服务器的公钥, 以确保只有指定服务器才能使用该陷门进行等值测试。

Huang 等^[13]提出授权密文等值测试 (PKE-AET), 方案中包含用户级别授权与密文级别授权 2 种模式, 不同模式生成的陷门不同, 分别可以对用户的所有密文或特定密文进行等值测试。授权陷门的生成同样需要用到第三方服务器的公钥。随后, Ma 等^[14]提出支持灵活授权的密文等值测试 (PKEET-FA), 包含 4 种类型授权模式的密文等值测试方案。Xu 等^[15]提出一种可验证的密文等值测试方案 (V-PKEET), 其中包含另外 2 种不同于文献[14]的授权模式。上述 3 个方案都只需进行一次加密, 便可给各个测试者 (如不同的第三方服务器) 分发特定授权模式的授权陷门, 测试者使用相应的测试算法进行等值测试。

3.2 基于身份的和无证书的密文等值测试方案

部分授权模式需要用到对方的公钥, 在执行密文等值测试方案之余还需要进行用户身份认证, 验证公钥的真伪性。在云环境中, 随着用户增多, CA 管理工作的负担也不断加重。

为解决证书管理问题, 使密文等值测试适用于云计算环境, Ma 在文献[16]首次提出基于身份的密文等值测试 (IBEET, identity-based encryption with equality test), 该方案将基于身份的加密 (IBE, identity-based encryption) 与密文等值测试技术进行结合, 用户不用提前确认彼此的公钥, 而是基于对方公开的 ID (如身份证号、邮箱地址等) 生成公钥, 进一步方便等值测试。在此基础上, Wu

等^[17]提出了新的 IBEET 方案, 可在确保安全性前提下有效节省计算开销。

为解决 IBEET 的密钥托管问题, Qu 等^[18]提出无证书的密文等值测试 (CL-PKEET), 用户使用自己选的一个秘密值生成公钥, 从 KGC 处得到私钥, 而授权陷门的生成需要用到私钥与秘密值。

3.3 基于属性的密文等值测试方案

为了实现更灵活的授权方式, 有研究人员尝试将基于属性的加密 (ABE, attribute-based encryption) 与密文等值测试技术进行结合, 实现基于属性的密文等值测试方案 (ABEET, attribute-based encryption with equality test), 如 Zhu 等^[19]的 KP-ABEET 与 Wang 等^[20]的 CP-ABEET 等。前者基于访问树, 而后者基于访问结构, 使某一群拥有特定属性的测试者可以执行测试算法, 不再需要向测试者逐个分发授权陷门, 也可以实现动态授权。但 Liao 等在文献[21]中提出前者的方案存在安全风险。随后, Cui 等^[22]设计了一个新的 CP-ABEET 方案, 具有更好的安全性以及更短的用户私钥。他们还设计了支持外包解密的属性基等值测试加密方案 (OCP-ABEET)^[23], 利用外包解密技术, 提高了客户端进行密文等值测试和解密算法的效率。

3.4 安全性提升的密文等值测试方案

绝大多数密文等值测试方案的安全性依赖于随机预言机模型。因此, 文献[24]借助分层的基于身份的加密 (hierarchical identity-based encryption) 实现了新的 PKEET 与 IBEET 方案, 并在标准模型下证明了方案的安全性。

考虑到对一些非法密文进行等值测试可能会导致数据泄露, Huang 等^[7]提出了密文过滤等值测试方案 (PKE-FET), 对可以进行测试的明文的数据域加以限制。在执行等值测试前进行范围判断, 被加密的明文在设定的数据域内才继续进行等值测试。该方案同样在标准模型下证明了安全性。

吴黎兵等^[25]指出目前的密文等值测试方案都基于单服务器, 可能会遭受内部关键字猜测攻击, 提出基于双服务器的密文等值测试方案 (DS-IBEET) 来解决这一问题, 并对计算性能与通信开销进行评估, 确保能在资源受限的移动设备上运行。

3.5 功能拓展的密文等值测试方案

Huang 等^[8]在文献[7]的基础上, 提出了标准模型下的 PKE-FET 方案, 并将其拓展为多关键字的 PEKS 方案, 实现密文等值测试技术与可搜索加密技术的结合。

Xu 等^[15]首次提出一种可验证的密文等值测试方案 (V-PKEET), 使用户可以校验密文等值测试的结果。考虑到某些云服务器可能是恶意的 (如被植入木马), 从而返回了错误的测试结果给用户, 在 V-PKEET 中, 服务器在返回结果之余还需返回一个凭证 (proof), 以供用户用于验证

测试结果。

Lin 等在文献[26]中借助拉格朗日插值公式给出了密文等值测试方案的一般性构造, 并将密文等值测试进行拓展, 提出签密等值测试 (SCET, signcryption with equality test)。

4 密文等值测试方案的比较

表 2 从安全性、安全模型、授权模式以及密钥的管理方式等方面给出了本文提到的若干典型密文等值测试方案的比较。

3.4 节归纳总结了目前密文等值测试技术

表 2 若干密文等值测试方案比较

方案名	Sec/wa	Sec/woa	模型	授权	密钥
PKEET ^[2]	—	OW-CCA	ROM	—	PKE
FG-PKEET ^[9]	OW-CCA	IND-CCA	ROM	4	PKE
AoN-PKEET ^[10]	OW-CCA	IND-CCA	ROM	1	PKE
ADG-PKEET ^[11]	OW-CCA	IND-CCA	ROM	4	PKE
PKE-DET ^[12]	OW-CCA	IND-CCA	ROM	1#	PKE
PKE-AET(1) ^[13]	OW-CCA	IND-CCA	ROM	1#	PKE
PKE-AET(2) ^[13]	OW-CCA	IND-CCA	ROM	2#	PKE
PKEET-FA(1) ^[14]	OW-CCA	IND-CCA	ROM	1	PKE
PKEET-FA(2) ^[14]	OW-CCA	IND-CCA	ROM	2	PKE
PKEET-FA(3) ^[14]	OW-CCA	IND-CCA	ROM	5	PKE
PKEET-FA(4) ^[14]	OW-CCA	IND-CCA	ROM	3	PKE
V-PKEET(1) ^[15]	OW-CCA	IND-CCA	ROM	1	PKE
V-PKEET(2) ^[15]	OW-CCA	IND-CCA	ROM	4	PKE
V-PKEET(3) ^[15]	OW-CCA	IND-CCA	ROM	6	PKE
PKE-FET ^[7-8]	IND-CCA	IND-CCA	SM	1	PKE
PKEET2 ^[24]	OW-CCA	IND-CCA	ROM	1	PKE
IBEET ^[16]	OW-ID-CCA	—	ROM	1	IBE
IBEET2 ^[17]	OW-ID-CCA	—	ROM	1	IBE
CL-PKEET ^[18]	OW-CCA	IND-CCA	ROM	1	IBE
IBEET3 ^[24]	OW-ID-CCA	IND-ID-CCA	ROM	1	IBE
DS-IBEET ^[25]	SS-CKA	—	ROM	1	IBE
KP-ABEET ^[19]	OW-CCA	T-CCA	ROM	1	ABE
CP-ABEET ^[20]	IND-ID-CPA	—	SM	1	ABE
CP-ABEET2 ^[22]	OW-CCA	IND-CCA	ROM	1	ABE
OCP-ABEET ^[23]	OW-CCA	IND-CCA	ROM	1	ABE

Sec/wa: 敌手获得陷门后该方案能达到的安全性; Sec/woa: 敌手未取得陷门时该方案能达到的安全性; OW: 单向性 (one-wayness); IND: 不可区分性 (indistinguishability); *-ID-CCA: 选择身份攻击与选择密文攻击 (chosen identity and chosen ciphertext attacks); *-ID-CPA: 选择身份攻击与选择明文攻击 (chosen identity and chosen plaintext attacks); SS-CKA: 选择关键字攻击下的语义安全 (semantic security under chosen keyword attacks); T-CCA: 选择密文攻击下可测试安全 (testable against chosen ciphertext attacks); ROM: 随机预言机模型; SM: 标准模型。

的6种授权类型,表中“授权”一栏中的数字是指该方案满足的授权类型的序号,带“#”表明还需要测试者(如服务器)的公钥。

可见,目前已有满足不同授权模式的PKEET方案,但只有用户级别授权模式的IBEET与ABEET方案。需要注意的是,ABEET方案中用户级别授权的陷门是与拥有特定属性的一群用户进行绑定,测试者获取陷门后,可以对拥有特定属性的所有用户的密文进行等值测试,不同于PKEET方案与IBEET方案中用户级别授权模式的陷门与用户本人绑定,且只能对该用户的密文进行等值测试。

此外,多数方案是在随机预言机模型下证明安全性,只有极少数方案^[8,20]在标准模型下得到证明。

5 密文等值测试技术应用场景

密文等值测试在云环境中有着广泛应用,以下总结了密文等值测试适用的若干场景。

1) 数据归档

在公司系统中,为了确保数据不泄露,发件人可能使用收件人的公钥对数据进行加密。若采用可搜索加密技术,系统受限于陷门生成方式,无法根据关键字对不同公钥加密的数据进行归档,但采用密文等值测试技术则可以给相同数据加上标签进行归档。

2) 用户数据删除

欧盟《通用数据保护条例》(General Data Protection Regulation)中再次提及“被遗忘权”,指用户可以要求网站管理者删除个人相关信息。考虑到社交网络中会出现涉及他人隐私信息的情况,基于密文等值测试技术可以将加密存储在数据库中他人提及自己的信息筛选以便删除。

3) 医疗系统

在医疗系统中,病人的病历或治疗方案是病人的隐私,需要加密保护。某些疾病在前期难以被发现,若通过病症比较,可能会发现潜在的疾病。由于使用的公钥不同,病人的加密病历无法进行有效对比,但使用密文等值测试技术可以筛选出患有相同病症的病人,而将治疗手段与疗效进行对比也可以挑选出该疾病最合适的治疗方案。此外,也可基于密文等值测试技术使有相同疾病的病人建立联系,彼此之间可以交流病情或相互鼓励。

4) 加密数据库

密文等值测试技术在加密数据库中也能发挥重要作用。在对数据检索的过程中,连接(JOIN)与自然连接(NATURAL JOIN)是常用的操作,对两张数据表中相同属性的相同数值进行操作。但当数据被加密时,两张数据表中同一个属性值通常被加密成不同的密文,使查询语句无法直接使用连接与自然连接操作。若结合密文等值测试技术,则可以实现加密数据库的跨表查询,在确保数据库安全性的同时对数据进行灵活操作。

6 结束语

目前密文等值测试技术已有不少研究成果,在医疗、商业等领域均有广阔的应用前景,但仍存在许多问题值得进一步研究与完善。如何构建安全高效且支持更多功能的密文等值测试方案仍是未来研究的重点与难点。

下面提出一些密文等值测试技术未来可研究的方向。

1) 批量进行等值测试

高效地进行批量等值测试算法是研究方向之一。目前的测试算法采取两两对比的形式,比较次数随着密文数目增长。目前的密文等值测试方案的比较算法计算量较大,在进行海量密文比较时需要花费大量时间。

2) 更多授权模式的IBEET方案

IBEET方案作为密文等值测试方案基于身份的拓展,具有较高的实用意义。然而,目前IBEET方案的授权模式均为用户级别授权,暂时没有其余5种级别授权的方案。支持灵活授权的IBEET方案可以使用户根据实际情况进行更加精确范围的授权。

3) 可撤销的授权

如何进行授权撤销是密文等值测试技术的一个难题。在密文等值测试方案中,测试算法所使用的授权陷门生成后交给测试者。一旦获取到授权陷门,测试者即可永久获得该授权级别的测试权限,并没有机制进行授权撤销。尤其是IBEET方案中,用户私钥基于用户ID生成,往往固定且难以改变,撤销机制更显得重要。

4) 安全模型

目前,密文等值测试方案的安全性证明采取

规约到困难问题的方式, 但绝大多数方案的安全性依赖于随机预言机模型。如何设计基于标准模型的密文等值测试方案是一个值得深入研究的问题。

5) 防止授权陷门泄露

授权陷门决定了测试者是否能进行等值测试、能进行什么授权级别的等值测试, 若授权陷门被泄露显然会造成一定程度的数据泄露。部分方案^[12,13]在设计时考虑到该问题, 授权陷门的生成需要用到测试者(如第三方服务器)的公钥, 但也增加了计算开销。

6) 更便捷的验证方式

可考虑设计一种高效便捷的验证算法。由于测试算法涉及的运算量较大, 往往采用外包的形式。但测试服务器可能在用户不知情的情况下被植入木马, 导致测试结果被篡改。文献[15]中提出了一种可验证的密文等值测试方案, 通过提供凭证的方式供用户验证, 但也增加了传输开销与计算开销。

参考文献:

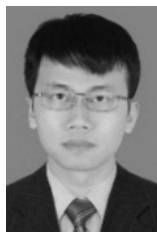
- [1] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2004: 506-522.
- [2] YANG G, TAN C H, HUANG Q, et al. Probabilistic public key encryption with equality test[C]//Cryptographers' Track at the RSA Conference. 2010: 119-131.
- [3] YONG H H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[C]//International Conference on Pairing-Based Cryptography. 2007: 2-22.
- [4] ZHAO F, NISHIDE T, SAKURAI K. Multi-user keyword search scheme for secure data sharing with fine-grained access control[C]//International Conference on Information Security and Cryptology. 2011: 406-418.
- [5] KIAYIAS A, OKSUZ O, RUSSELL A, et al. efficient encrypted keyword search for multi-user data sharing[M]// Computer Security-ESORICS 2016. 2016: 173-195.
- [6] LI Z, ZHAO M, JIANG H, et al. Multi-user searchable encryption with a designated server[J]. Annals of Telecommunications, 2017, 72(9/10):1-13.
- [7] HUANG K, CHEN Y C, TSO R. Semantic secure public key encryption with filtered equality test PKE-FET[C]//12th International Joint Conference on e-Business and Telecommunications (ICETE). 2015, 4: 327-334.
- [8] HUANG K, 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.
- [9] TANG Q. Towards public key encryption scheme supporting equality test with fine-grained authorization[C]//Australasian Conference on Information Security and Privacy. 2011: 389-406.
- [10] TANG Q. Public key encryption supporting plaintext equality test and user specified authorization[J]. Security and Communication Networks, 2012, 5(12): 1351-1362.
- [11] TANG Q. Public key encryption schemes supporting equality test with authorisation of different granularity[J]. International Journal of Applied Cryptography, 2012, 2(4): 304-321.
- [12] MA S, ZHANG M, HUANG Q, et al. Public key encryption with delegated equality test in a multi-user setting[J]. The Computer Journal, 2015, 58(4): 986-1002.
- [13] HUANG K, TSO R, CHEN Y C, et al. PKE-AET: public key encryption with authorized equality test[J]. The Computer Journal, 2015, 58(10): 2686-2697.
- [14] MA S, HUANG Q, ZHANG M, 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.
- [15] 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.
- [16] MA S. Identity-based encryption with outsourced equality test in cloud computing[J]. Information Sciences, 2016, 328: 389-402.
- [17] WU L, ZHANG Y, CHOO K K R, et al. Efficient and secure identity-based encryption scheme with equality test in cloud computing[J]. Future Generation Computer Systems, 2017, 73: 22-31.
- [18] QU H, YAN Z, LIN X J, et al. Certificateless public key encryption with equality test[J]. Information Sciences, 2018, 462: 76-92.
- [19] ZHU H, WANG L, AHMAD H, et al. Key-policy attribute-based encryption with equality test in cloud computing[J]. IEEE Access, 2017, 5: 20428-20439.
- [20] WANG Q, PENG L, XIONG H, et al. Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing[J]. IEEE Access, 2018, 6: 760-771.
- [21] LIAO Y, CHEN H, LI F, et al. Insecurity of a key-policy attribute based encryption scheme with equality test[J]. IEEE Access, 2018, 6: 10189-10196.
- [22] CUI Y, HUANG Q, HUANG J, et al. Ciphertext-policy attribute-based encrypted data equality test and classification[J]. Cryptology ePrint Archive, 2018.
- [23] CUI Y, HUANG Q, HUANG J, et al. Outsourced ciphertext-policy attribute-based encryption with equality test[C]//Proceedings of Inscrypt, Lecture Notes in Computer Science. Springer. 2018.
- [24] LEE H T, LING S, SEO J H, et al. Public key encryption with equality test in the standard model[J]. IACR Cryptology ePrint Archive, 2016: 1182.
- [25] 吴黎兵, 张宇波, 何德彪. 云计算中基于身份的双服务器密文等

值判定协议[J]. 计算机研究与发展, 2017, 54(10): 2232-2243.

WU L B, ZHANG Y B, HE D B. Dual server identity-based encryption with equality test for cloud computing[J]. Journal of Computer Research and Development, 2017, 54(10): 2232-2243.

- [26] LIN X J, SUN L, QU H. Generic construction of public key encryption, identity-based encryption and signcryption with equality test[J]. Information Sciences, 2018, 453: 111-126.

[作者简介]



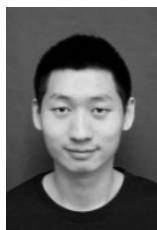
王元昊 (1994-), 男, 广东潮州人, 华南农业大学硕士生, 主要研究方向为信息安全、可搜索加密。



崔钰钊 (1994-), 男, 河南商丘人, 华南农业大学硕士生, 主要研究方向为信息安全、应用密码学、公钥可搜索加密。



郭庆文 (1993-), 男, 广东揭阳人, 华南农业大学硕士生, 主要研究方向为信息安全、数字签名、零知识证明。



李宏博 (1991-), 男, 山东青岛人, 华南农业大学博士生, 主要研究方向为可搜索加密、公钥等值测试加密、基于身份加密。



黄琼 (1982-), 男, 江西南昌人, 华南农业大学教授、博士生导师, 主要研究方向为密码学与信息安全。