从云邮件安全看加密技术的发展

徐 鹏[1,2], 陈天阳[1], 金 海[1]

[1]服务计算技术与系统教育部重点实验室 集群与网格计算湖北省重点实验室 计算机学院 华中科技大学, 武汉 中国 430074
[2]深圳华中科技大学研究院, 深圳 中国 518057

摘要 随着云计算的快速发展, 与云邮件系统相关的安全问题越来越受到人们的关注。传统公钥加密技术虽然可以满足云邮件系统的安全性需求, 但是在易用性方面却存在严重不足。通过分析传统加密技术存在的不足, 探讨前沿的代理重加密和可搜索公钥加密技术在解决云邮件系统的安全性与易用性方面的优势与存在的科学问题。

关键词 云邮件; 安全; 基于身份加密; 代理重加密; 广播加密; 可搜索加密
中图法分类号 TN915.08 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.01.007

The Development of Encryption Techniques for Cloud Email Security

XU Peng[1,2], CHEN Tianyang[1], JIN Hai[1]

[1] Services Computing Technology and System Lab, Cluster and Grid Computing Lab, School of Computer, HuaZhong University of Science and Technology, Wuhan 430074, China
[2]Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518057, China

Abstract Along with the rapid development of cloud computing system, the security problems of cloud mail system has attracted many attentions. These problems can be solved by the traditional public-key encryption techniques, but they make the resulted cloud email system inconvenient for users. This paper analyzes the limitations of the tradition encryption techniques, introduces the advantages of some advanced encryption techniques, like proxy re-encryption and searchable public key encryption, and discusses the still existing problems of these techniques.

Key words Cloud mail; security; Identity-Based Encryption; Proxy Re-Encryption; Broadcast Encryption; Searchable Encryption

1 引言

云邮件系统是一种以软件即服务模式向各公司或机构提供邮件服务的云计算系统。它的基本架构如图 1 所示。在云邮件系统中, 云邮件服务提供商提供已经配置好的邮件系统供用户租用, 用户只需要自己架设管理服务器, 对云邮件系统进行参数设置及管理系统用户等。云邮件厂商通常会在一台物理服务器上部署多台虚拟服务器, 同时对外提供服务。

近年来, 云邮件系统的发展十分迅速, 如图 2 所示为 Radicati 对云邮件企业总营收的预测结果。由图可以看到, 从 2014 年, 云邮件系统的市场规模以每年大约 42%的比例高速发展; 而到 2018 年, 所有云邮件企业的总营收会增长到 16.9 亿美元。另据 DataMotion 的调查, 有 50%的企业用户正在使用云邮件系统, 或者有使用云邮件系统的计划。除此之外, Gartner 还预计, 在 2017 年底, 至少 33%的企业用户会使用云邮件系统来为自己提供邮件服务。这一切都说明了云邮件系统发展受到广泛关注。

云邮件系统受到企业青睐的主要因素是租用云平台所带来的低廉成本。如表 1 所示为 Proofpoint 发起的一项关于云邮件服务节省成本数量调查的结果。从表中可以看到, 虽然用户数量越多, 云邮件系统能节省的成本也越高, 但是当用户数量比较少的

通讯作者: 徐鹏, 博士, 副教授, Email: xupeng@mail.hust.edu.cn。
本课题得到国家自然科学面上基金(No.61472156)、国家重点基础研究发展计划(973 项目, No.2014CB340600)与深圳市基础研究(学科布局)项目(No. JCYJ20170413114215614)资助。
收稿日期: 2017-04-18; 修改日期: 2017-08-10; 定稿日期: 2017-12-05

表 1 Proofpoint 关于云邮件服务节省企业成本数量的调查结果[2]

Table 1 Survey about the cost saved through Cloud Mail for enterprises producted by Proofpoint[2]

用户数量	存储技术	自建邮件服务器成本(包含人力成本)	使用云邮件系统的成本	总计节省成本
5,000	NAS	$2,108,300	$1,097,488	48%
10,000	CAS	$23,259,600	$1,986,232	92%
20,000	CAS	$45,829,200	$3,634,976	93%
30,000	CAS	$69,357,200	$5,454,975	93%

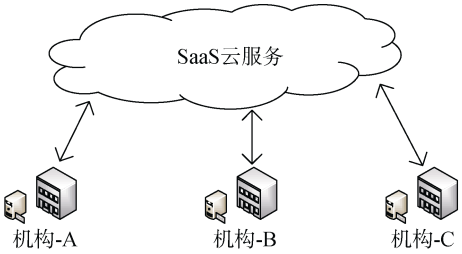

图 1 云邮件系统的具体架构

Figure 1 Architecture of Cloud Mail System

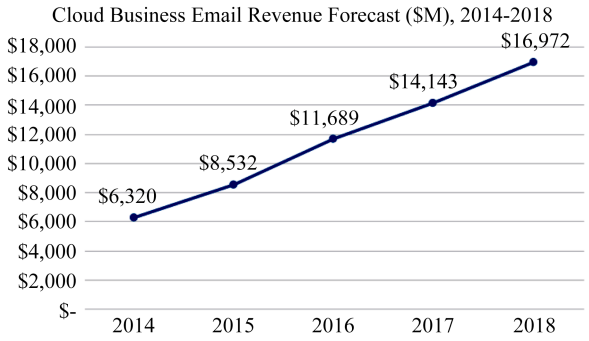

图 2 Redicati 对云邮件市场的预测[1]

Figure 2 Redicati`s prediction on market of the Cloud Mail[1]

时候, 云邮件系统节省的成本总数也是不小的数字。除了成本之外, 企业使用云邮件系统还有另外一个重要原因, 就是不需要去关注邮件系统中软件的更新、系统的漏洞以及数据的备份等。这些重要但琐碎的事务都由云邮件服务提供商提供解决方案。同时, 如果云邮件系统中的数据出现了问题, 企业或者机构可以向云邮件服务提供商寻求赔偿, 从这一点上来说, 使用云邮件系统, 公司的邮件数据也有了一定保障。

虽然云邮件系统的发展如此迅速, 但是因为担忧安全问题, 还是有大量用户对于云邮件系统顾虑重重。用户的担忧不是没有道理, 毕竟电子邮件承载了用户太多的隐私甚至机密信息, 并且近年来电子邮件服务器的泄露事故层出不穷。比如 2016 年美国大选期间的邮件泄露事件; 2013 年沃尔玛内部邮件泄露事件; 2012 年叙利亚总统办公室邮件泄露事件以及 2009 年哥本哈根气候变化会议邮件泄露事件等。这些邮件泄漏事件都对当事人或者当事国家造成了不小的损失, 从这些案例可以看出, 邮件服务器的安全非常重要。而在云邮件系统中, 常常是一台物理服务器为多个公司或者机构提供服务, 这也意味着在云邮件系统厂商的单台服务器上, 往往有多个公司或者机构的邮件信息。如果这些服务器上的邮件被泄露出去, 将会影响到不止一家公司, 造成的损失也会因为波及范围的扩大而变得无法估量, 甚至可能对云邮件系统的发展造成毁灭性的影响。因此, 将加密技术应用在云邮件系统上去是很有必要的。虽然传统加密技术可以保证邮件的安全性, 但是在商用云邮件系统上, 安全性仅仅是最基础的要求。本文将以云邮件系统为背景介绍加密技术的发展, 并且分析这些加密技术依然存在的科学问题。

2 传统的云邮件加密技术

2.1 基于 SSL 的云邮件系统

基于安全套接字层(Secure Socket Layer, SSL)的云邮件系统是使用 SSL 协议来传递邮件。SSL 协议的运行原理如图 3 所示, 其具体运行步骤为:

1. 用户与服务器通讯, 以协商一个用于对通信链路进行加密的对称密钥(或称会话密钥);

2. 用户使用会话密钥加密邮件, 然后将加密后的邮件传递给邮件服务器;

3. 收到加密的邮件后, 服务器会将邮件解密, 再将其存储到用户的发件箱, 并投递给对应的收件人。目前, 提供 SSL 技术的邮件公司有 Voltage、DataMotion、Proofpoing、EdgeWave、Symantec、Sophos、LuxSci 和 Privato 等。

从 SSL 协议的运行方式中, 我们可以发现, 基于 SSL 的云邮件系统中, 用户的邮件在服务器端和客户端都是明文保存的, 只有在传输链路上才是加密的。这种的技术的好处是实现简单, 运行起来效率高, 用户群发邮件和群转发邮件的操作简单, 占用客户端的带宽和计算资源小, 并且在云邮件服务器上对邮件进行内容检索也很简单。但是, 这种加密技术只能防止攻击者对通信链路的窃听, 而不能保证邮件

保存时的安全。如果云邮件服务器遭到攻击, 用户邮件泄露, 那么攻击者会获得用户的全部明文邮件。2011 年 Gmail 便发生了这种邮件泄露事故。除此之外, 这种加密技术也不能避免邮件服务器对用户邮件的扫描与窥探, 造成用户隐私泄露, 比如 2013 年, Gmail 就承认其扫描用户邮件内容, 不尊重用户隐私。因此, 这种加密技术的安全性是不足的。

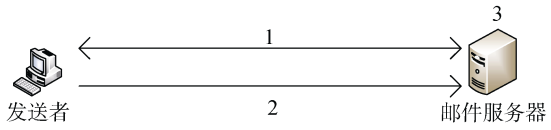

图 3　SSL 协议的运行原理
Figure 3　SSL Procotol

2.2　基于 PGP/IBE 的云邮件系统

PGP(Pretty Good Privacy, 一种基于 RSA 公钥加密体系的邮件加密协议)协议与基于身份加密[3](Identity-Based Encryption, IBE)均属于公钥加密体制, 在运行原理上比较相似。图 4 为 PGP 协议的运行原理, 其具体运行步骤为:

1. 发件人请求 CA 证书, 验证收件人公钥;

2. 发件人利用收件人公钥加密邮件, 并发送给服务器;

3. 收件人从服务器接收解密邮件, 解密出明文。

图 5 为 IBE 的运行原理, 其具体运行步骤为:

1. 发件人用收件人 ID 加密邮件, 并发送给服务器;

2. 收件人从服务器接收加密的邮件, 用私钥解密并查看。

目前, 提供 PGP 技术的邮件公司有 Voltage、DataMotion、Cryptzone、Symantec、Sophos 和 Privato 等; 提供 IBE 技术的邮件公司有 Voltage、DataMotion、Proofpoint 和 Trendmicro 等。

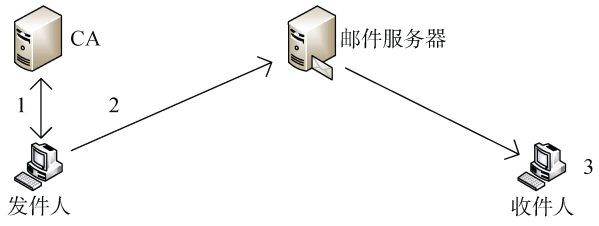

图 4　PGP 协议的运行原理
Figure 4　PGP Protocol

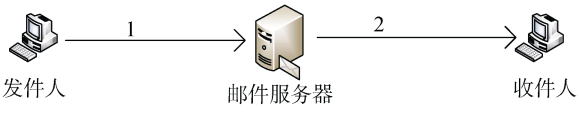

图 5　IBE 协议的运行原理
Figure 5　IBE Protocol

相比于 SSL 协议, PGP/IBE 协议的优点是更加安全。因为这两种协议是用接收者的公钥对邮件内容进行加密, 而加密后的密文只有拥有私钥的接收者才能解密。也就是说, 使用这种加密方式, 用户无需担心自己的邮件被攻击者拦截获取或者被服务器偷窥扫描, 因为他们都没有私钥, 无法获得明文。虽然这两种加密方式提高了邮件系统的安全性, 有效保障了用户的隐私, 但是它们也有自己的缺点。

首先在发送邮件时, 如果用户要将一份邮件发送给多个收件人, 那么有多少个收件人, 用户的客户端就要将用户的邮件加密多少次, 然后将这些密文再分别传送到云邮件服务器上。因此, 对于群发邮件, 客户端的加密运算会消耗用户过多的时间; 上传邮件到服务器的过程也会消耗用户的时间与带宽资源; 另外, 如果用户在发送邮件时使用的是移动设备, 那么用户的电量也会因为加密时的运算开销与上传文件时的通信开销而快速消耗, 降低用户设备的续航。

除了上面两点之外, PGP 与 IBE 更严重的问题是, 它们不支持群转发功能。也就是说, 如果这两种加密体制下的云邮件系统用户在云邮件服务器上有一封早先发送过的邮件想要转发给其他用户, 那么他就必须先从云邮件服务器上将要转发的邮件下载到本地, 将其解密后再重新加密发送出去。这样的邮件转发过程既复杂又浪费用户的时间, 当然也存在上面所说的消耗用户电量的问题。因此, 从上面所说的缺点来看, PGP 与 IBE 并不能很好的满足用户需要。

从上述 SSL、PGP 与 IBE 协议的介绍可以看出, 传统加密技术使得云邮件的安全性与用户使用时的友好性无法兼顾。

3　加密云邮件的群发和群转发

针对传统公钥加密技术无法有效实现加密邮件的群发和群转发问题, 代理重加密[4](Proxy Re-Encryption, PRE)成为解决思路之一。PRE 技术可以让云端直接对密文进行计算, 将仅某用户可以解密的密文直接转化成另一个用户可以解密的密文, 从而节省大量网络资源, 也充分利用了云端的计算资源, 减少了用户的负担。

稍具体地说, PRE 的主要流程有:

1. 用户 A 用自己的公钥加密数据, 并将密文存放到云端, 此密文数据只能由用户 A 用自己的私钥解密, 从而实现数据的云存储保密性;

2. 当用户 A 需要将此密文数据共享给用户 B 时, 用户 A 可以生成一个重加密密钥, 并将其发送给云端;

3. 云端使用该重加密密钥对密文进行计算, 将仅可以由用户 A 解密的密文转化为用户 B 可以解密的密文, 且在转化的过程中不会泄露明文的任何信息。

3.1 PRE 的相关工作

PRE 的思想是由 Blaze, Bleumer 和 Strauss 在文献[4]中提出的, 并在文献[5]中进行了规范的形式化定义。由于 PRE 在密文共享方面的优越性, 研究人员近几年来对 PRE 开展了大量的研究, 主要的工作如下。

3.1.1 传统公钥体制的 PRE 方案

在没有使用双线性映射的情况下,文献[6]提出的 PRE 方案实现了选择密文攻击(Chosen Ciphertext Attacks, CCA)下的安全性。基于使用最广泛的 RSA 签名, 文献[7]构造了 PRE 方案。文献[8]所提出了单向并具有 CCA 安全性的 PRE 方案, 其中“单向”是指接收者的加密数据不会被同时共享给发送者。文献[9-11]提出的 PRE 方案在实现安全性的同时也实现了匿名性。在传统的公钥体制中, 每个用户的公钥为一个随机数, 因此用户公钥与用户本身并没有天然的绑定关系, 可能会发生由于公钥与用户不相符引起的数据泄露问题。因此, 在实际应用中需要权威的 CA 为每一个用户生成一个证书从而绑定用户及其公钥。每次执行加密算法时, 发送方都要从 CA 下载证书, 并验证用户及其公钥是否匹配; 当用户数量较大时, 整个系统的证书管理、下载和验证过程会带来很大开销[12]。为了解决传统公钥体制所面临的问题, 出现了一种特殊的公钥体制, 即 IBE, 进而也提出了基于身份加密体制的 PRE 方案。

3.1.2 基于身份加密体制的 PRE 方案

文献[13]所提方案在随机预言机(Random Oracle, RO)模型下具有可证明安全性。文献[3]所提方案在标准模型下具有可证明安全性, 比 RO 模型下的方案具有更强的安全性。文献[14,15]所提方案在标准模型下具有 CCA 安全性。文献[3]所提方案中的初始密文、重加密密钥和重加密密文都具有常数级长度, 使其传输效率更高, 并且将此方案运用到了医疗健康领域, 在应用上做了很大的突破。

在上述基于传统公钥体制的代理重加密方案和基于身份的代理重加密方案中, 代理方为每个接收者生成一条密文, 在多接收者请求一条数据的情况下, 需要为每一个接收者生成一个重加密密钥, 代理方使用此重加密密钥为每一个接收者执行重加密算法生成一条重加密密文。因此执行此步骤的次数与接收者人数成正比, 在这种情况下会造成大量的计算资源和网络资源消耗。在实际的应用场景中, 多接收者请求一条数据的情况非常常见, 热门资源经常被大批量地分享, 这样上述问题在这种场景下会非常明显。

为了解决这个问题, 一般会使用广播加密(Broadcast Encryption, BE)。BE 是指为多接收者加密一条数据, 生成一条密文, 此密文可被所有指定的接收者用自己的私钥解密, 非指定的接收者无法解密。在这种方法中, 批量的用户请求可以只进行一次加密。为了具有广播的特点, 文献[15]提出了广播代理重加密(Broadcast PRE, BPRE)方案。BPRE 的工作模式和常规的代理重加密很相似, 但是它有更强大的功能。在 BPRE 中, 发送者可以为一个接收者集合生成一条初始密文, 而不用为每一个接收者生成一条初始密文。而且, 发送者可以为另一个收者集合生成一个代理重加密密钥, 发送给代理方做计算, 然后只生成一条重加密密文, 这条重加密密文可以由这个接收者集合中的每个成员解密。广播代理重加密方案很好地解决了多用户请求初始密文所面临的效率问题, 在运行过程中由于发送方只需要生成一个重加密密钥, 因此会节省大量的计算和网络资源。

在以上提出的这些代理重加密方案中, 在代理收到发送者的重加密密钥后, 可以将发送者的所有初始密文进行重加密运算, 这样发送方也因此失去了共享的细粒度控制能力, 使得云端重加密的密文范围超出用户的预期。为了解决这个问题, 文献[16]提出了基于类型的代理重加密(Type-based PRE,PRE)方案, 使得代理方只能对具有指定类型的初始密文做重加密计算。文献[17]中提出了一个相似的概念, 即带条件的代理重加密(Conditional PRE, CPRE)。在这种方法中, 当且仅当初始密文具有的条件与重加密密钥所具有的条件相同时, 云端才可以对该初始密文进行重加密计算。上述两种方案都在 RO 模型下具有可证明安全性。之后, 更多的 CPRE 方案被提出。文献[3,14,18]所提方案均实现了对密文的细粒度控制。文献[19]所提方案实现了基于身份体制、细粒度控制和代理重加密的有效结合, 并且提出的方案在标准模型下具有 CCA 安全性。文献[20]提出了具有 CCA 安全性的 CPRE 方案, 并且使其运算过程更高效。文献[21]提出了具有匿名性的带条件的广播代理重加密方案, 并且提出的方案在标准模型下具有可证明安全性。

文献[22]所提方案可以允许发送者控制对自己初始密文做重加密运算的时间。当发送者为重加密一条初始密文生成一个重加密密钥时, 发送者需要将这条初始密文的接收者作为输入。在实际情况中,

这意味着发送者需要保存他所发送的所有初始密文的接收者, 这对存储资源的限的终端(例如移动设备)来说, 有很大的限制。

文献[23,24]所提方案具有多用户间双向重加密的特性, 这种特性使一条密文可被多次重加密, 也就是说一个重加密密钥可被两方共享。举例来说, 如果 Alice 为 Bob 生成了一个重加密密钥, 代理方可使用此重加密密钥将 Alice 的密文计算生成一个可以由 Bob 解密的密文, 此重加密密钥也可以用做将 Bob 的密文为 Alice 生成重加密密文。这两个方案分别在随机预言机模型和标准模型下具有抵抗密文攻击的安全性。文献[25]所提方案具有在云计算环境下可撤销的基于身份代理重加密的特性, 这种特性支持用户可以授权或撤销对密文的解密权。

上述 PRE 方案, 在易用性和高效性方面依然存在问题: 1. 用户生成重加密密钥发送给云端后, 云端可以使用此重加密密钥将发送者的所有密文数据进行转化, 因此用户无法对云端转化的密文数据进行粒度控制; 2. 传统的公钥体制在运行过程中, 需要认证中心将用户与证书进行绑定, 用户需要进行证书管理和证书认证, 造成管理消耗; 3. 当需要向多用户分享时, 只能为一个接收者生成一个重加密密钥, 因此需要生成的密文数目与接收者人数成正比, 会造成时间和网络资源的大量消耗。

针对这些问题, 我们提出了带条件的基于身份广播代理重加密(Conditional Identity-based Broadcast Proxy Re-Encryption, CIBPRE)方案[19]。

3.2　CIBPRE 方案

CIBPRE 方案有三个特点: 基于身份加密、广播加密和带条件的代理重加密。它们的作用如下:

1. 基于身份加密, 意味着 CIBPRE 加密体制的运行不需要公钥基础设施(Public Key Infrastructure, PKI)的支持, 因为用户的邮件地址就是加密时所需的公钥, 只需要密钥生成中心(Key Generation Centre, KGC)为每个用户生成私钥即可。而 KGC 的运行成本比 PKI 要低许多, 并且客户端在加密时免去了获取公钥证书的开销。因此 CIBPRE 加密体制运行所需要的成本比较小;

2. 广播加密, 意味着用户可以方便地群发邮件。用户在使用广播加密技术群发加密邮件时, 只要将明文邮件使用所有收件人的邮箱地址加密一次, 产生的密文就可以被所有收件人使用自己的私钥解密。广播加密技术克服了 PGP 协议和 IBE 协议在群发邮件时加密开销与通信开销大的问题, 节约了用户的时间和带宽, 提升了移动设备用户的续航;

3. 带条件的代理重加密, 意味着用户可以方便地群转发自己保存在云邮件服务器上面的邮件。当用户想要转发一封已经存在于服务器上的邮件给其他一组接收者的时候, 他只需要在本地生成一个重加密密钥文件再将其提交给服务器。服务器在收到重加密密钥后就可以对用户指定的邮件进行重加密操作, 完成后再将重加密后的邮件转发给用户新指定的一组接收者。新的接收者在收到重加密后的邮件后, 便可以使用自己的私钥解密出明文来查阅了。同时, 由于使用了带条件的代理重加密技术, 云服务器也不可能和某接收者合谋, 利用用户的重加密密钥重加密用户的所有邮件, 造成用户隐私泄露。

CIBPRE 加密体制的核心算法有 7 个, 它们分别为 $Setup_{\mathrm{PRE}}$、$Extract_{\mathrm{PRE}}$、Enc_{PRE}、$RKExtract_{\mathrm{PRE}}$、$ReEnc_{\mathrm{PRE}}$、$Dec\text{-}1_{\mathrm{PRE}}$ 和 $Dec\text{-}2_{\mathrm{PRE}}$。它们的作用如下:

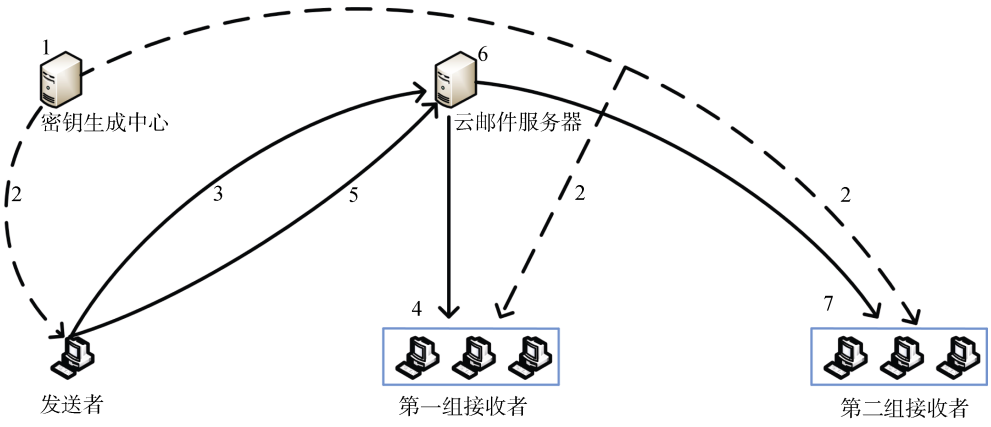

图 6　基于 CIBPRE 体制的邮件系统运行原理

Figure 6　CIBPRE-Based Cloud Mail system

1. $Setup_{PRE}$: 初始化 CIBPRE 系统并生成系统运行所必要的参数;

2. $Extract_{PRE}$: 根据用户 ID 为用户生成私钥;

3. Enc_{PRE}: 对用户的文件进行加密操作, 产生的密文可被一组接收者解密;

4. $RKExtract_{PRE}$: 生成重加密密钥, 用于重加密已有邮件;

5. $ReEnc_{PRE}$: 利用重加密密钥对用户的邮件进行重加密操作, 产生的重加密邮件可被另一组接收者解密;

6. $Dec\text{-}1_{PRE}$: 利用私钥解密 Enc_{PRE} 算法加密的邮件;

7. $Dec\text{-}2_{PRE}$: 利用私钥解密 $ReEnc_{PRE}$ 算法重加密后的邮件。

如图 6 所示为基于 CIBPRE 加密体制的云邮件系统的运行原理。

基于 CIBPRE 的云邮件系统运行时, 其具体的运行步骤为:

1. 密钥生成中心运行 $Setup_{PRE}$ 算法, 初始化并生成主公开参数与主秘密参数;

2. 密钥生成中心运行 $Extract_{PRE}$ 算法, 为系统中的用户生成私钥;

3. 发送者运行 Enc_{PRE} 算法, 使用第一组接收者的 ID 加密邮件, 并将其上传到邮件服务器;

4. 第一组接收者上线时, 从邮件服务器下载加密邮件到本地, 并在本地运行 $Dec\text{-}1_{PRE}$ 算法, 解密并查看邮件密文;

5. 发送者要将已发送的邮件转发给第二组接收者时, 会在本地运行 $RKExtract_{PRE}$ 算法, 生成重加密密钥, 并上传到云邮件服务器;

6. 云邮件服务器收到发送者的重加密密钥后, 利用重加密密钥对指定的邮件运行 $ReEnc_{PRE}$ 算法, 并将重加密后的邮件转发给指定的接收者;

7. 第二组接收者上线时, 从邮件服务器下载重加密的邮件到本地, 并在本地运行 $Dec\text{-}2_{PRE}$ 算法, 解密并查看邮件明文。

表 2 CIBPRE 方案与现有邮件加密技术的对比

Table 2 Comparisons between CIBPRE and the existing email-encryption schemes

特性	CIBPRE	SSL	PGP/IBE
对单一邮件的公钥加密	支持	不支持	支持
加密邮件群发	只需发送一封加密邮件	只需发送一封邮件	需对邮件多次加密并分别发送
加密邮件群转发	只需提交一次重加密密钥	只需发送一封邮件	需对邮件解密, 再多次加密并分别发送

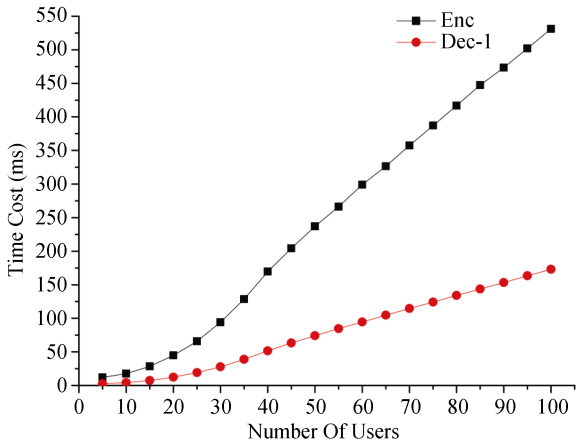

图 7 初始密文加解密性能开销与用户数量关系[19]

Figure 7 The decryption cost of an initial cipher[19]

3.3 CIBPRE 方案性能开销与功能对比

如图 7 所示为加密生成初始密文(折线 Enc)和解密初始密文(折线 Dec-1)时, CIBPRE 方案性能开销与用户数量的关系; 如图 8 所示为对密文进行重加密操作(折线 ReEnc)与解密重加密密文(折线 Dec-2)时, CIBPRE 方案性能开销与用户数量的关系。如表 3 所示为测试的环境。从测试结果可以看出, CIBPRE 方案运算所需时间与系统中支持的收件人数量大致成正比, 并且当收件人数量不是特别高时, 对初始密

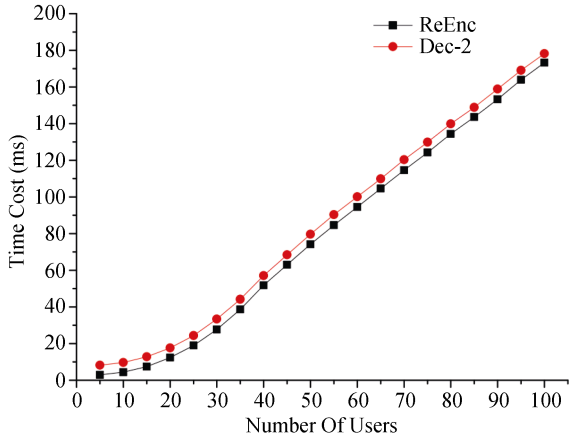

图 8 重加密密文加解密性能开销与用户数量关系[19]

Figure 8 The decryption cost of a re-encrypted cipher[19]

表 3 性能测试环境[19]

Table 3 Configurations and parameters[19]

CPU	Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz
操作系统	CentOS 6.7 x64
编译环境	gcc pbc library
	椭圆曲线参数
椭圆曲线	$y^2=x^3+x$
椭圆曲线基于的有限域 F_q	q=87807107996633125224377819847540498158068831994142082110286533992664756308802229570786251794226622214231558587695823174592777133673174813249251299982247 91
嵌入度	2
群阶	730750818665451621361119245571504901405976559617

文以及重加密密文的加解密操作所耗费的时间都在可以接受的范围内。

如表 2 所示为 CIBPRE 方案与 SSL、PGP/IBE 方案的综合对比。从表中可以看出, CIBPRE 方案既拥有 SSL 协议的便捷性, 又拥有 PGP/IBE 协议的安全性。再加上其可接受的性能开销, 可以得出 CIBPRE 加密体制非常适合应用在云邮件系统的结论。

4 加密云邮件系统的云检索

虽然上面介绍的 CIBPRE 方案可以在保障安全性的条件下有效提高用户体验, 但它还是摆脱不了加密邮件系统普遍都有的缺点, 即在云邮件服务器上无法按照内容来检索所需邮件。这个缺点产生的原因也很直接, 即加密后的邮件密文通常不支持搜索。假设用户在云服务器存储了几百封密文邮件, 用户想要取回特定的一封邮件时, 由于云端没有检索功能, 不能找到用户想要的邮件, 只能将全部邮件都返回给用户, 用户解密后自行检索才能得到想要的数据。很显然, 这种处理方法在实际应用中是不能被接受的, 所以如何实现用户提交检索请求时, 云服务器能高效率检索并返回指定的密文是云邮件系统的重要问题和需求之一。

为了解决该问题, 可搜索加密(Searchable Encryption, SE)被提出。总的来说, 可搜索加密方案允许数据拥有者用加密密钥生成可搜索密文, 并将密文存放在云端; 当数据拥有者需要委托云端检索含有指定关键字的密文时, 数据拥有者用解密密钥和被检索关键字生成对应的检索陷门, 并将该陷门发送给云端; 收到陷门后, 云端可以检索匹配的密文, 并返还给数据拥有者; 最后, 数据拥有者解密出明文。在上述过程中, 可搜索加密方案可以保障被检索关键字的保密性。

4.1 SE 的相关工作

可搜索加密方案有两种: 可搜索对称加密(Searchable Semantic Encryption, SSE)[26]与可搜索公钥加密(Public-Key Encryption with Keyword Search, PEKS)[27], 其中, 因为可搜索对称加密需要与其他用户共享秘密消息的天然缺陷, 不适合应用在主要为收件人提供云检索服务的云邮件系统中。因此在这里不讨论可搜索对称加密。

可搜索公钥加密由 Dan Boneh 在文献[27]首次提出, 之后其相关研究受到了广泛的关注。针对 PEKS 的概念存在的一些缺陷, Abdalla 等人[28]进一步完善了 PEKS 的一致性定义, 并且解决了 PEKS 与基于身份加密间的通用转换问题。围绕 PEKS 的检索多样性问题, 文献[29-35]实现了关键字的合取检索; 文献[36-38]实现了关键字的范围检索; 文献[37]实现了关键字的子集检索; 文献[31, 39]实现了时间范围检索; 文献[39, 40]实现了关键字的相似度检索。针对不可信的关键字检索陷门生成者, Camenisch 等人[41]提出了“不经意的”关键字陷门生成算法, 从而保护关键字在其检索陷门生成过程中的隐私性。

虽然上述文献都为 PEKS 的研究与发展作出了重要贡献, 但是所有上述 PEKS 方案均存在安全性高(具有语义安全性)但是检索效率低下问题, 即检索复杂度与所有密文的数目线性相关。为了实现关键字的高效检索, Bellare 等人[42]引入了“确定的公钥加密”这一概念, 并且形式化地定义其安全性。该安全性比单向性强, 但是比语义安全性弱。在检索效率方面, 确定的公钥加密使得关键字的检索十分高效, 其检索效率就如同关键字没有进行加密一般。Bellare 等人[42]同时也提出了一个确定的公钥加密方案(即 RSA-DOAEP 方案), 和一个在 RO 模型下将概率的公钥加密方案转化成确定的公钥加密的通用方法。针对文献[42]中确定的公钥加密方案存在的安全性不足, Bellare 等人[43]和 Boldyreva 等人[44]分别在标准模型下提出了确定的公钥加密方案。前者基于通用的难题假设给出了通用的构造方法, 后者基于具体的难题假设给出了效率更高的实例化方案。进一步地, Brakerski 等人[45]提出了具有更好安全性的确定的公钥加密方案。由于在理论上, 只有当明文空间具有先验高熵时, 确定的公钥加密方案才可能具有语义安全性, 否则攻击者只需要发起加密并且测试这种简单的暴力攻击就可以提取出加密的内容。因此, 由于关键字空间通常不具有先验高熵, 因此由确定的公钥加密实现的关键字可搜索公钥加密无法实现语义安全性。

Camenisch 等人[41]非正式地描述了一种方法, 使得具有相同关键字的密文形成一条隐式链。如果服务器正确查找到第一条匹配的密文, 他们的方法将会提高检索的效率。然而, 他们并没有解决如何找到第一段匹配密文的问题。同时, 他们的加密方案不具备语义安全性。在每一条链中, 第一段密文和后边的密文是平凡可区分的。这种平凡可区分性使得在这个方案中很难正确定义语义安全性。实际上, 他们并没有提供任何正式的安全性定义。

Boneh 等人[27]在公钥加密开山作中给出了明确的安全性定义, 即选择关键字攻击下的语义安全性(Semantic Security under Chosen Keyword Attacks, SS-CKA)。此安全性定义意味着如果服务器没有得到关键字检索的自陷门, 那么服务器就不会获取含有对应关键字的密文段中的任何信息。但是选择关键字攻击下的语义安全性并没有论述当关键字检索自陷门被知晓的情况下是否依旧能保障关键字的机密性。

Byun 等人[46]首次提出了关键字猜测攻击(Keyword Guessing Attacks, KGA)这个概念。Jeong 等人[47]证明了任何至少满足计算不可区分的一致性的 PEKS 方案都容易遭受 KGA 这种攻击。KGA 的攻击模式, 即攻击者产生所有对应关键字的密文。如果关键字空间是多项式规模, 那么这种攻击模式非常容易实现。为了抵抗外部攻击者发起的 KGA 攻击, 文献[48,49]分别提出两种方法: 一种是为关键字检索陷门建立安全性的传输信道; 另一种是 PEKS 的发送方和接收方通过协商关键字的别名实现关键字的匿名性。但是, 由于 PEKS 的主要优点在于发送方和接收方不需要同时在线即可以完成可搜索密文的生成, 因此文献[49]提出的方案在实际应用失去了 PEKS 天生的优势。解决这个问题的一个简单方法就是通过允许发送者自定义关键字实现增大关键字的空间。然而, 正如文献[50]所示, 这种方式使得接收者很难去生成对应的关键字检索陷门。并且如果不同的发送者使用不同的关键字来表达同一个意思, 那么接收者就必须生成多个关键字检索陷门来检索匹配的密文, 由此带来巨大的计算开销。因此, 很有必要拓展传统的 PEKS 模型来实现在关键字空间很小的情况下, 保证在 KGA 攻击模式下关键字的机密性[51]。文献[52]拓展了 PEKS, 将静态索引以及动态索引结合起来构造了混合索引密文检索方案, 利用静态索引将关键字的首次检索复杂度从 O(n)降低到 O(n*w), 利用动态索引将关键字的非首次检索复杂度从 O(n)降低到 O(w)。

根据上面的国内外研究现状的阐述可以看出, 在可搜索对称加密领域, “结构化”的思想已经被用来实现了高安全的和检索高效的关键字可搜索对称加密, 并进一步实现结构化数据的对称加密。但是, 在可搜索公钥加密领域, “结构化”的思想仅在文献[41]中出现, 但是这篇文章完全没有讨论其提出方案的高安全性, 而且很明显的该方案不具有高安全性。进一步地, 该文献也没有正式地和形式化地讨论和定义结构化可搜索公钥加密及其安全性。仅针对 PEKS 的低检索效率, 有一些文献[42-45]虽然提出了高检索效率的方法, 但同时也大幅降低了安全性。由此可见, 有关“结构化可搜索公钥加密”及其相关领域的研究几乎是没有的, 结构化数据的公钥加密研究更是难觅踪迹。

由于 PEKS 具有的高安全性使得即使含有相同关键字的两个密文, 它们之间也相互独立, 因此 PEKS 的检索复杂度似乎必须是线性级(即与密文的总量线性相关)。而且, 现有的高安全的 PEKS 实例化方案也都是这种线性级的检索复杂度。为了解决这个问题, 我们提出了一种带隐藏结构的可搜索公钥加密方案[53](Searchable Public-key Ciphertext with Hidden Structures, SPCHS)。

4.2 SPCHS 方案

SPCHS 首次在保证语义安全性的条件下实现了亚线性级的检索复杂度, 降低了 PEKS 方案的检索开销。除此之外, 通过采用我们提出的一种特殊的基于身份密钥封装机制[53], 提出了新的匿名基于身份广播加密方案[54], 该方案具备基于标准模型常数级解密效率、抗适应性攻击以及强匿名性这四种特性。SPCHS 方案的核心思路是, 为同一个关键字的所有可搜索密文构造一个隐藏的链式结构, 再将所有的链式结构的头部与一个公共头部连接起来, 形成一个星型结构, 如图 9 所示。

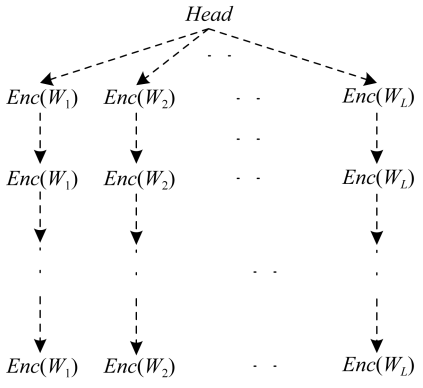

图 9 SPCHS 方案为可搜索密文构造的星型结构[50]

Figure 9 Star-like structure of ciphers in SPCHS[50]

SPCHS 方案的核心算法有 5 个, 它们分别是参数初始化算法 *SystemSetup* 、隐藏结构初始化算法 *StructureInitialization* 、可搜索密文生成算法 *StructuredEncryption* 、关键字检索陷门生成算法 *Trapdoor* 和结构化密文检索算法 *StructuredSearch* , 它们的作用是:

1. *SystemSetup*: 初始化 SPCHS 方案运行所需的参数, 包括主公开信息和主秘密信息;

2. *StructureInitialization*: 本算法接收 SPCHS 的主公开信息, 生成并初始化隐藏结构的私有部分与公有部分;

3. *StructuredEncryption*: 本算法接收 SPCHS 的主公开信息、关键字和隐藏结构的私有部分, 生成 SPCHS 的可搜索密文;

4. *Trapdoor*: 本算法接收 SPCHS 的主秘密信息和关键字, 生成关键字检索陷门;

5. *StructuredSearch*: 本算法接收系统公钥、隐藏结构的公有部分、可搜索密文集合和关键字搜索陷门, 查找到关键字对应的密文。

如图 10 所示为基于 SPCHS 的内容可搜索加密邮件系统的运行原理。

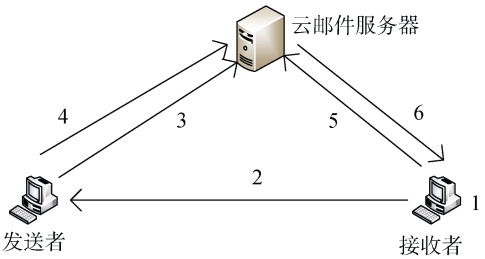

图 10　基于 SPCHS 可搜索加密的邮件系统运行原理
Figure 10　SPCHS-Based mail system

它的具体运行步骤为:

1. 接收者输入安全参数, 运行 *SystemSetup* 算法, 生成系统主公开信息和主秘密信息;

2. 接收者将主公开信息传递给发送者, 发送者运行 *StructureInitialization* 算法, 生成隐藏结构的公有部分和私有部分; 发送者将在步骤 2 中生成的隐藏结构的公有部分上传至云邮件服务器;

3. 发送者为接收者生成可搜索密文时, 输入系统主公开信息、密文的关键字和隐藏结构的私有部分, 运行 *StructuredEncryption* 算法, 生成可搜索密文, 并上传到服务器保存;

4. 接收者要根据某关键字查找发送者发送给自己的文件时, 输入系统主秘密信息和待检索的关键字, 运行 *Trapdoor* 算法生成关键字检索陷门, 并上传至服务器;

5. 服务器收到接收者的关键字检索陷门后, 对每一个发送可搜索密文给接收者的发送者, 输入系统主公开信息、发送者隐藏结构的公有部分、可搜索密文和检索陷门, 运行 *StructuredSearch* 算法, 找到所有满足条件的密文;

6. 将第 5 步找到的满足条件的密文返回给接收者。

4.3　SPCHS 的性能开销与功能对比

如图 11 所示为 SPCHS 方案性能开销与含有指定关键字的密文数量的关系图像; 如表 4 所示为测试环境。可以看到, SPCHS 方案的检索用时与包含指定关键字的密文的数量成正比关系。如果不考虑极端情况, 如检索的关键字正好被云存储服务器上所有密文都包含, 那么相比 PEKS 方案, SPCHS 方案能够节省的时间将会非常可观。

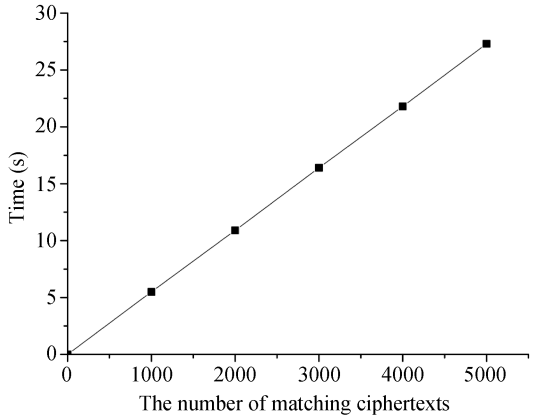

图 11　检索耗时与指定关键字密文数量关系[50]
Figure 11　The search cost[50]

SPCHS 方案在保证了可搜索公钥加密安全性的基础上, 提高了密文检索效率, 如果能够应用在云邮件系统上, 可以极大地提升用户体验, 提高用户的使用效率。

5　跨异构密码算法的加密云邮件系统

在使用上述技术提高云邮件系统的安全性和易用性的同时, 也带来了另一个问题, 即两个使用不同加密体制的云邮件系统的用户间该如何互相转发邮件的问题。这个问题具有重要的实用意义, 现代社会, 企业间的合作司空见惯, 而两个不同企业的员工之间也大多使用 email 进行通信交流。如果这两个企业的同时使用了云邮件系统, 并且这两个企业的云邮件系统使用的加密体制不一样, 那两个企业的员工间如何互相转发邮件便成为问题。对于 SSL 协

议, 解决这个问题比较简单, 因为 SSL 协议中, 云平台上的邮件以明文形式保存, 在进行邮件转发时云邮件系统直接将邮件投递到另一个云邮件系统即可。虽然很便捷, 但是 SSL 协议的安全性不足, 无法阻止邮件明文的泄露。对于 PGP/IBE 协议, 解决这个问题便很困难了, 因为 PGP/IBE 只有在指定的密码体制下使用私钥才能解密, 直接转发到另一个体制的云邮件系统中, 接收者是没有办法解密出明文的。同样的, 基于 PRE 的云邮件系统也存在同样的问题。针对异构 PRE 方案之间的安全邮件发送问题, 学术界提出了混合代理重加密(Hybrid Proxy Re-Encryption, HPRE)。

表 4 性能测试环境[50]

Table 4 Configurations and parameters[50]

CPU	Intel CPU E5300 @ 2.60GHz
编译环境	Win XP, Microsoft VC++ 6.0
密码学库	MIRACL version 5.4.1
椭圆曲线参数	
椭圆曲线	$y^2 = x^3 + A \cdot x + B \cdot x$
基础五项式	$t^m + t^a + t^b + t^c + 1$
基域: 2^m	$m = 379$
A	1
B	1
群阶: q	$2^m + 2^{(m+1)/2} + 1$
a	315
b	301
c	287

近几年来, 为了满足加密云数据的多样化共享功能, 国内外已经涌现出多种多样的 PRE 方案。这些方案在具备代理重加密的基本功能基础上, 还具有很多其他的特性, 从而使之能够满足不同应用场景的要求。从密钥类型方面来看, 有传统的基于证书的 PRE 方案、基于身份的 PRE 方案和基于属性的 PRE 方案等; 从功能性方面来看, 有带条件的 PRE 方案[15,21]能够实现以细粒度的方式安全共享用户的云端数据; 广播 PRE 方案[15, 22]可同时向多个用户共享数据。

这些种类繁多的 PRE 方案有利于用户共享他们在云端的数据。然而, 带来便利的同时也产生了一个新的问题: 假设有两个加密云存储平台分别使用了不同的 PRE 方案, 那么这两个云存储平台之间就无法安全共享数据。这个问题同样存在于同一个云平台中, 当两个企业租用了同一云平台, 但是了不同的 PRE 方案来实现它们的云存储服务时, 也无法实现安全的数据共享。

为了实现异构 PRE 方案之间的安全数据共享, 学者们提出了混合代理重加密方案(Hybrid PRE, HPRE)。2007 年, Matsuo 在 Pairing-Based Cryptography 会议上首次提出了 HPRE 的概念[55], 并提出了 CB-PRE 到 IB-PRE 的密文转换 HPRE 方案。Niu 等人[56]在 Matsuo 的基础上做了改进, 解决了其存在的密钥托管问题。Wang 等人[57]提出了 IB-PRE 到 CB-PRE 的 HPRE 方案, 但存在密钥托管问题。针对该问题, Zhang 等人[58]提出了解决方案。Wei 等人[59]和 Mizuno 等人[60]分别提出了 CL-PRE 到 AB-PRE, 和 AB-PRE 到 IB-PRE 的 HPRE 方案。Tang 等人[61]研究了跨域的 PRE 问题, 即授权方与被授权方分别处于不同的两个域中(部署了不同 IB-PRE 方案), 并提出了跨域的 IB-PRE 到 IB-PRE 的 HPRE 方案来解决该场景的问题。Xu 等人[62]提出了安全的 IB-PRE 到 CB-PRE 的 HPRE 方案, 并且该方案实现了数据的细粒度共享。

现有的 HPRE 方案均是针对特定的 PRE 方案, 无法通用地解决异构 PRE 方案之间的的数据转换, 因而, 我们提出了通用混合代理重加密[63](Generally HPRE, GHPRE)来更好地解决异构 PRE 方案间的数据共享。

5.1 GHPRE 方案

GHPRE 提供了一种在任意两个不同的 PRE 体制间, 或者由 PRE 体制向传统公钥加密体制(Public Key Encryption, PKE)进行文件分享的通用方案。由于 GHPRE 方案的通用性极强, 在两个加密体制不同的云邮件系统间部署 GHPRE 方案时不需要对已部署的加密体制进行太多修改, 只要按照 GHPRE 的定义添加代码即可。因此 GHPRE 方案非常适合应用在两个已有的加密体制不同的云邮件系统之间。

这里, 首先给出 PRE 和 PKE 的定义。PKE 由以下算法组成:

1. $Setup_\alpha$: 初始化并生成 PKE 系统运行所需的参数;

2. $Extract_\alpha$: 为系统中的每个用户生成一对公私钥;

3. Enc_α: 利用用户公钥对数据进行加密, 加密后的文件能且仅能被公钥对应的私钥解密;

4. Dec_α: 利用用户的私钥解密使用用户公钥加密的数据。

PRE 由以下算法组成:

1. $Setup_\beta$: 初始化并生成 PRE 系统运行所需的参数;

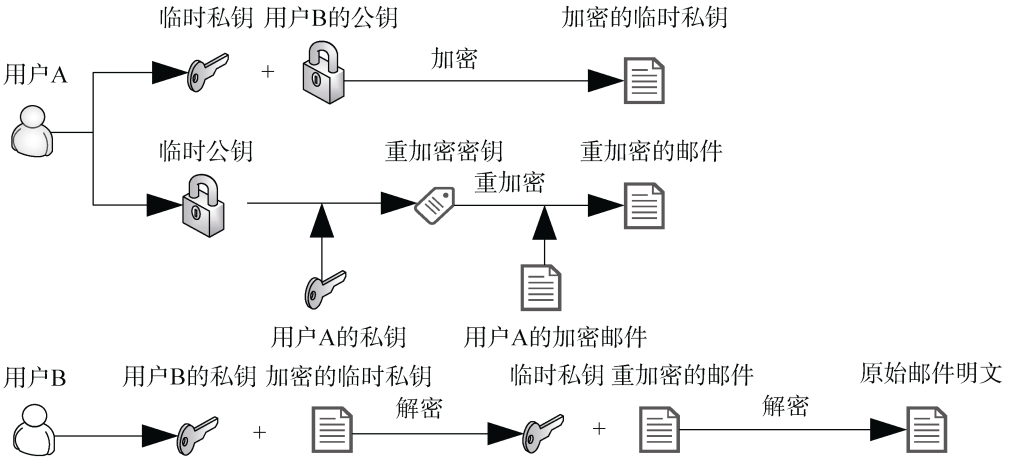

图 12　GHPRE 算法的核心流程

Figure 12　GHPRE scheme

2. $Extract_{\alpha}$: 为系统中的每个用户生成一对公私钥;

3. Enc_{β}: 利用用户公钥将明文数据进行加密, 生成 PRE 系统的初始密文, 生成的密文能且仅能利用公钥对应的私钥被 $Dec\text{-}1_{\beta}$ 解密出明文; $Dec\text{-}1_{\beta}$: 利用用户的私钥, 解密使用用户公钥加密的密文, 生成明文;

4. RK_{β}: 生成密文的重加密密钥。用户将重加密密钥上传到云端, 云端利用重加密密钥, 使用 $ReEnc_{\beta}$ 算法对用户指定的密文进行重加密, 生成重加密密文。重加密密文可以被在重加密密钥生成过程中指定的一个用户解密;

5. $ReEnc_{\beta}$: 利用重加密密钥, 对用户指定的文件进行重加密操作, 生成重加密密文。重加密密文可以被在重加密密钥生成过程中指定的一个用户解密;

6. $Dec\text{-}2_{\beta}$: 使用用户的私钥解密 $ReEnc_{\beta}$ 算法生成的重加密密文, 生成对应的明文。

GHPRE 是一套通用的算法, 它的核心算法流程如图 12 所示。假设一个 PRE 体制的用户 A 要向另外一个 PKE 体制的用户 B 转发一封邮件 $Mail$, 且邮件 $Mail$ 是使用用户 A 的公钥 PK_A 加密存储在云端的。用户 A 首先从自身的密钥生成中心 KGC_A 获取一对临时公私密钥(PK_{Temp} , SK_{Temp}), 随后使用自己的私钥 SK_A 和临时公钥 PK_{Temp} 在本地生成用于在用户 A 所在的 PRE 体制内部进行加密文件共享的重加密密钥 RK_A。之后, 用户 A 向其所在的云邮件系统提交生成的重加密密钥 RK_A, 由云端使用 RK_A 将用户原本的密文邮件 $EncMail$ 重加密, 得到重加密后的密文邮件 $ReEncMail$。其中, $ReEncMail$ 可以使用临时私钥 SK_{Temp} 进行解密。用户 A 查询获得用户 B 的公钥 PK_B, 随后使用公钥 PK_B 将可以解密邮件的临时私钥 SK_{Temp} 加密为密文 $EncSK$ 待用。云邮件服务器 $Cloud_A$ 再将($EncSK$, $ReEncMail$)一起传输给用户 B 所属的云邮件服务器 $Cloud_B$。传输完毕后, 用户 B 只需要从云服务器 $Cloud_B$ 上下载($EncSK$, $ReEncMail$), 再使用自己的私钥从 $EncSK$ 中解密出临时私钥 SK_{Temp}, 使用 SK_{Temp} 解密 $ReEncMail$ 就可以顺利获得用户 A 的邮件明文 $Mail$。

由 GHPRE 算法的核心流程可以看出, 算法很巧妙地申请了一对临时的公私钥, 发送者在跨密码体制转发邮件时, 相当于把自己的邮件转发给了临时的公钥, 再用接收者的公钥将临时私钥加密。这样一来, 接收者就可以先解密出临时私钥, 再使用临时私钥解密出明文了。

接下来阐述如何使用 GHPRE 方案来进行解决异构密码算法的加密云邮件系统间的邮件转发问题。假设部署了基于 PKE 的 α 和基于 PRE 的 β 两个加密云邮件系统, 下面详细阐述如何部署 GHPRE 方案(称为 γ), 实现 β 系统中的用户 Alice 发送邮件给 α 系统中的用户 Carl, 其中令 β = ($Setup_{\beta}$, $Extract_{\beta}$, Enc_{β} , $Dec-1_{\beta}$, RK_{β} , $ReEnc_{\beta}$, $Dec-2_{\beta}$) 和 α = ($Setup_{\alpha}$, $Extract_{\alpha}$, Enc_{α} , Dec_{α})。

假设 Alice 想要发送邮件给 Carl。令 γ = ($Setup_{\gamma}$, $Extract_{\gamma}$, Enc_{γ} , $Dec-1_{\gamma}$, RK_{γ} , $ReEnc_{\gamma}$, $Dec-2_{\gamma}$), γ 是一个 GHPRE 方案, 采用了 PRE 方案 β 和 PKE

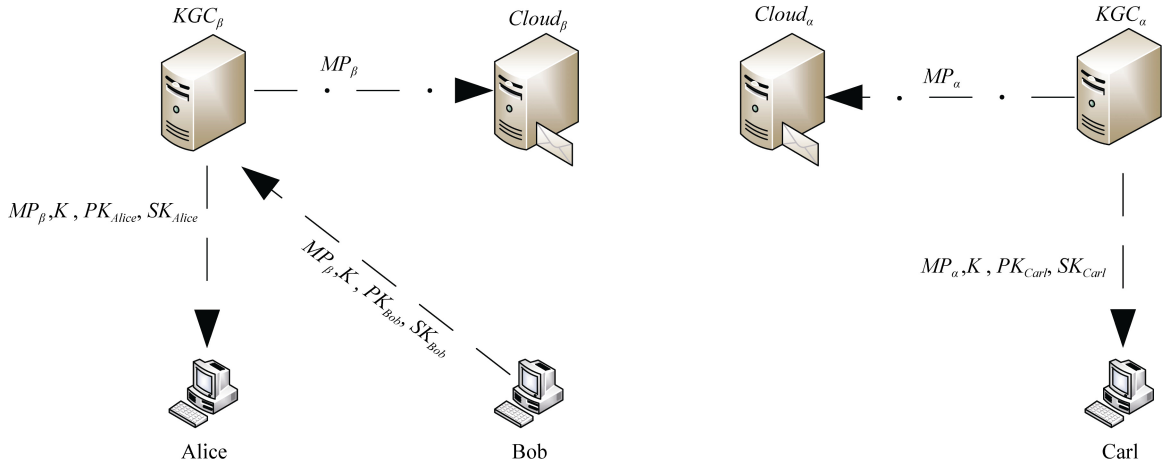

图 13 GHPRE 系统初始化与密钥分发过程

Figure 13 System setup and key publish in GHPRE

方案 α 作为构造模块。方案 γ 的主公开参数 $MP_\gamma = (MP_\alpha, MP_\beta)$。$\beta$ 系统中的用户发送邮件给与 α 系统中的用户由以下几个步骤组成:

1. 系统初始化阶段: β 加密云和 α 加密云均生成它们各自的主公开和主秘密参数, 从而初始化各自的系统。令 KGC_β 和 KGC_α 分别是 β 加密云和 α 加密云的密钥生成中心。令(K, SE, SD)为一个对称加密方案, 其中 K 是对称密钥空间, SE 和 SD 分别是对称加密和解密算法。KGC_β 执行算法 $Setup_\beta$ 生成主公开和主秘密参数(MP_β, MS_β), 并选择一个安全的对称加密方案(K, SE, SD), 比如 AES 算法。类似地, KGC_α 执行算法 $Setup_\alpha$ 生成主公开和主秘密参数(MP_α, MS_α)。最后, KGC_β 发布 (MP_β, K)给 β 加密云 $Cloud_\beta$, KGC_α 发布 MP_α 给 α 加密云 $Cloud_\alpha$。这一步骤如图 13 中点虚线所示;

2. 密钥分发阶段: KGC_β 和 KGC_α 为各自系统中的用户生成一对真实的公私钥。Alice 想要加入 β 加密云时, 然后 KGC_β 执行算法 $Extract_\beta$ 生成一对真实的公私钥(PK_{Alice}, SK_{Alice})并通过一个安全信道将$(MP_\beta, K, PK_{Alice}, SK_{Alice})$发送给 Alice。同样的, Bob 通过同样的方式获取他的真实公私钥(PK_{Bob}, SK_{Bob})。当 Carl 加入 α 加密云时, KGC_α 执行算法 $Extract_\alpha$ 生成一对真实公私钥(PK_{Carl}, SK_{Carl})并通过安全信道将$(MP_\alpha, PK_{Carl}, SK_{Carl})$发送给 Carl。这一步骤如图 13 的虚线所示;

3. Alice 生成一个重加密密钥 $RK_{\gamma,Alice\to Carl} \leftarrow RK_\gamma$ 并将其发送给 $Cloud_\beta$。在这一步, 首先 Alice 从 KGC_β 获取一对临时公私钥(PK_{Temp}, SK_{Temp})以及 α 系统的主公开参数 MP_α; 接着, Alice 执行算法 RK_β 生成 β 系统的重加密密钥 $RK_{\beta,Alice\to PK_{Temp}}$, 并执行算法 Enc_α, 用 Carl 的公钥将临时私钥加密得到 $EncSK_{Carl}$; 最后, Alice 将 γ 的重加密密钥 $RK_{\gamma,Alice\to Carl} = (RK_{\beta,Alice\to PK_{Temp}}, EncSK_{Carl})$发送给 β 邮件系统。这一步骤如图 14 中的点虚线所示;

4. β 邮件系统得到重加密密钥 $RK_{\gamma,Alice\to Carl} = (RK_{\beta,Alice\to PK_{Temp}}, EncSK_{Carl})$, 执行重加密算法 $ReEnc_\gamma$ 将 Alice 的密文 $EncMail_{Alice}$ 重加密得到新密文 $ReEncMail_{PK_{Temp}}$, 并将$(ReEncMail_{PK_{Temp}}, EncSK)$发送给 $Cloud_\alpha$。这一步骤如图 14 中的虚线所示;

5. 当 Carl 上线时, 他从 $Cloud_\alpha$ 收到邮件密文$(ReEncMail_{PK_{Temp}}, EncSK)$, 然后先执行 $Dec-2_\gamma$ 得到用于解密邮件的对称密钥 K_{Alice}, 再执行 SD 得到明文数据 $Mail$。在一步中, Carl 先执行 Dec_α 得到临时私钥 SK_{Temp}, 接着执行 $Dec-2_\beta$ 得到对称密钥 K_{Alice}, 最后执行 SD 得到邮件明文。这一过程如图 14 中的实线所示。

从上述 γ 的应用可以看出, γ 可以非常便利地部署到正在运行的 PRE 系统 β 中。Alice 需要重加密原密文时, 并不需要修改存在云端的密文。另外, 用户与 KGC 之间的通信量与数据共享的请求量呈线性

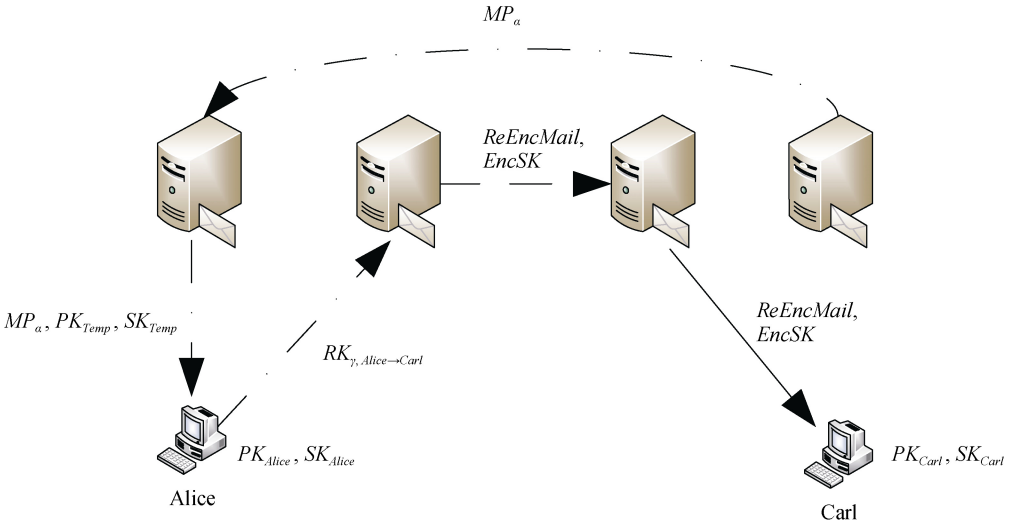

图 14　GHPRE 分享文件过程
Figure 14　File sharing in GHPRE

关系。要降低通信开销, 用户在共享数据给同一个人时可以使用同样的公私钥对。这就使得用户与 KGC 之间的通信量仅与数据消费者的数量线性相关了。这个方法的唯一缺陷就是会增加用户管理临时密钥的负担。

CIBPRE 提供了从一个 PRE 体系向另一个 PRE 体系, 或由 PRE 体系向 PKE 体系进行安全文件共享的解决方案。虽然在目前的 PKI 体系下, 本方案并不具有很高的实用性, 但是它清除了 PRE 加密体系间安全文件共享的障碍, 为未来 PRE 加密体系做了重要的铺垫。

6　垃圾邮件的云过滤

加密技术的发展提升了邮件系统用户的安全性和用户体验, 同时也提高了垃圾邮件的隐蔽性。关于垃圾邮件的危害, 人们已经讨论了很长时间了, 其最主要的危害就是浪费用户时间、降低用户体验、占用服务器带宽与存储空间以及可能携带恶意软件等。

现在防范垃圾邮件的主要方式是根据发件地址拦截和在邮件系统上根据邮件内容过滤。其中, 根据发件地址拦截的方式很容易误伤正常用户的邮件, 并且垃圾邮件的发送者也可以很容易地伪造或更换发件地址, 因此根据发件地址拦截的方式有一定局限性。根据内容过滤垃圾邮件的方法可以很好地工作在无加密的或以 SSL 作为加密技术的云邮件系统上, 因为邮件服务器可以直接扫描邮件的明文。但是在基于 PGP/IBE/PRE 的邮件系统上无法发挥作用。在这些云邮件系统上, 只有接收者才能看到邮件的明文, 服务器无法分辨哪些邮件是垃圾邮件。目前, 还没有一种方法可以基于邮件内容解决加密邮件的垃圾过滤问题。

7　总结

本文从云邮件系统上的邮件安全开始, 讨论了传统的 SSL 协议在安全性上的缺陷, 以及 PGP 和 IBE 协议在群发和群转发功能上的不足。接着, 介绍了既能保证用户邮件的安全性, 又可以让用户便捷地群发邮件和群转发邮件的 CIBPRE 方案, 并介绍了 CIBPRE 方案在云邮件系统上的典型应用。接下来, 讨论了可以实现在云邮件服务器进行加密邮件检索的可搜索加密方案, 介绍了在保证检索关键字安全的基础上, 提升了传统 PEKS 检索效率的 SPCHS 方案。以上都是在同一个云邮件系统下, 提高用户安全性和用户体验的方法, 这些方案对在两个异构加密云邮件系统之间进行邮件转发的情况则无能为力。此时就需要使用 GHPRE 方案实现异构密码算法的云邮件系统之间的邮件转发功能。最后, 介绍了加密云邮件系统中解决难度最大的加密垃圾邮件的过滤问题。要想彻底解决这个问题, 我们面临的挑战还非常多。

参考文献

[1] “Cloud business email market, 2014-2018”, Radicati Group, http://www.radicati.com/wp/wp-content/uploads/2014/10/Cloud-Business-Email-Market-2014-2018-Executive-Summary.pdf, Oct, 2014

[2] “Cloud-based archiving vs. on-premises legacy archiving”, Proofpoint Group. (2012), http://video.proofpoint.com/id/cloud-based-archiving-vs.-on-premises-legacy-archiving-TCO-white-paper, Jun,

2012.

[3] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, “A type-and- identity-based proxy re-encryption scheme and its appli-cation in healthcare,” in Proc. 5th VLDB Conf. Secure Data Manage, pp. 185–198, 2008.

[4] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., pp. 127–144, 1998.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Trans. Inf. Syst. Security, vol. 9, pp. 1–30, 2006.

[6] R. H. Deng, J. Weng, S. Liu, and K. Chen, “Chosen-ciphertext secure proxy re-encryption without pairings,” Cryptol. Netw. Security, vol. 5339, pp. 1–17, 2008.

[7] V. Kirtane and C. P. Rangan, “RSA-TBOS signcryption with proxy re-encryption,” in Proc. 8th ACM Workshop Digital Rights Manage, pp. 59–66, 2008.

[8] B. Libert and D. Vergnaud, “Unidirectional chosen-ciphertext secure proxy re-encryption,” in Proc. 11th Int. Workshop Practice Theory, pp. 360–379, 2008.

[9] J. Shao and Z. Cao, “CCA-secure proxy re-encryption without pairings,” in Proc. 12th Int. Conf. Practice Theory Public Key Cryptography, pp. 357–376, 2009.

[10] G. Ateniese, K. Benson, and S. Hohenberger, “Key-private proxy re-encryption,” in Proc. Cryptographers’ Track RSA Conf. Topics Cryptol, pp. 279–294., 2009.

[11] J. Shao, P. Liu, G. Wei, and Y. Ling, “Anonymous proxy reencryption,” Security Commun. Netw., vol. 5, no. 5,pp. 439–449, 2012.

[12] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi, “A closer look at PKI: Security and efficiency,” in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, pp. 458–475, 2007.

[13] M. Green and G. Ateniese, “Identity-based proxy re-encryption,” in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, pp. 288–306, 2007.

[14] C.-K. Chu and W.-G. Tzeng, “Identity-based proxy re-encryption without random oracles,” in Proc. 10th Int. Conf. Inf. Security, pp. 189–202, 2007.

[15] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, “Conditional proxy broadcast re-encryption,” in Proc. 14th Australasian Conf. Inf. Security Privacy, pp. 327–342, 2009.

[16] Q. Tang, “Type-based proxy re-encryption and its construction,” in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol, pp. 130–144, 2008.

[17] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, “Conditional proxy re-encryption secure against chosen-ciphertext attack,” in Proc. 4th Int. Symp. Inf., Comput. Commun.Security, pp. 322–332, 2009.

[18] J. Shao, G. Wei, Y. Ling, and M. Xie, “Identity-based conditional proxy re-encryption,” in Proc. IEEE Int. Conf. Commun, pp. 1–5, 2011.

[19] P. Xu, T. Jiao, Q. Wu, W. Wang and J. Hai, “Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email” *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-78, Jan. 2016.

[20] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, “Efficient conditional proxy re-encryption with chosen-ciphertext security,” in Proc. 12th Int. Conf. Inf. Security, pp. 151–166 , 2009.

[21] L. Fang, W. Susilo, and J. Wang, “Anonymous conditional proxy re-encryption without random oracle,” in Proc. 3rd Int. Conf. Provable Security, pp. 47–60, 2009.

[22] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, “A conditional proxy broadcast re-encryption scheme supporting timedrelease,” in Proc. 9th Int. Conf. Inf. Security Practice Experience, pp. 132–146, 2013.

[23] R. Canetti and S. Hohenberger, “Chosen-ciphertext secure proxy reencryption,” in Proc. 14th ACM Conf. Comput. Commun. Security, pp. 185–194, 2007.

[24] T. Matsuda, R. Nishimaki, and K. Tanaka, “CCA proxy re-encryption without bilinear maps in the standard model,” in Proc. 13th Int. Conf. Practice Theory Public Key Cryptography, pp. 261–278, 2010.

[25] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, ” An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing,” in Proc. Eur. Symp. Res. Comput. Security, pp. 257–272, 2014.

[26] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in *Proc. IEEE S&P*, pp. 44–55, May.2000.

[27] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer-Verlag, pp. 506–522, 2004.

[28] M. Abdalla *et al.*, “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,” in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 3621, V. Shoup, Ed. Berlin, Germany: Springer- Verlag, pp. 205–222, 2005.

[29] D. J. Park, K. Kim, and P. J. Lee, “Public key encryption with conjunctive field keyword search,” in *Information Security Applications* (Lecture Notes in Computer Science), vol. 3325, C. H. Lim and M. Yung, Eds. Berlin, Germany: Springer-Verlag, pp. 73–86, 2005.

[30] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword

search over encrypted data," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 3089, M. Jakobsson, M. Yung, and J. Zhou, Eds. Berlin, Germany: Springer-Verlag, pp. 31–45, 2004.

[31] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in *Information and Communications Security* (Lecture Notes in Computer Science), vol. 3783, S. Qing, W. Mao, J. López, and G. Wang, Eds. Berlin, Germany: Springer-Verlag, pp. 414–426, 2005.

[32] J. Baek, R. Safavi-Naini, W. Susilo, Public Key Encryption with Keyword Search Revisited, ICCSA 2008, LNCS, vol. 5072, pp. 1249-1259, Springer, Heidelberg (2008)

[33] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *PairingBased Cryptography—Pairing* (Lecture Notes in Computer Science), vol. 4575, T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, Eds. Berlin, Germany: Springer-Verlag, pp. 2–22, 2007.

[34] E.-K. Ryu and T. Takagi, "Efficient conjunctive keyword-searchable encryption," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops*, pp. 409–414, May 2007.

[35] Mitsuhiro Hattori, Takato Hirano, Takashi Ito, Nori Matsuda, Takumi Mori, Yusuke Sakai, Kazuo Ohta, "Ciphertext-Policy Delegatable Hidden Vector Encryption and Its Application to Searchable Encryption in Multi-user Setting", IMA Int. Conf., pp. 190-209, 2011.

[36] J. Bethencourt, T.-H. H. Chan, A. Perrig, E. Shi, and D. Song, "Anonymous multi-attribute encryption with range query and conditional decryption," School Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-CS-06-135, 2006.

[37] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in *Proc. IEEE S&P*, vol. 4392, S. P. Vadhan, Ed. Berlin, Germany: Springer-Verlag, pp. 350–364, May 2007.

[38] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of Cryptography* (Lecture Notes in Computer Science), pp. 535–554, 2007.

[39] D. W. Cheung, N. Mamoulis, W. K. Wong, S. M. Yiu, and Y. Zhang, "Anonymous fuzzy identity-based encryption for similarity search," in *Algorithms and Computation* (Lecture Notes in Computer Science), vol. 6506, O. Cheong, K.-Y. Chwa, and K. Park, Eds. Berlin, Germany: Springer-Verlag, pp. 61–72, 2010.

[40] Saeed Sedghi, Peter van Liesdonk, Svetla Nikova, Pieter H. Hartel, Willem Jonker, "Searching Keywords with Wildcards on Encrypted Data," SCN 2010, pp. 138-153, 2010.

[41] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in *Public Key Cryptography— PKC* (Lecture Notes in Computer Science), vol. 5443, S. Jarecki and G. Tsudik, Eds. Berlin, Germany: Springer-Verlag,pp. 196–214, 2009.

[42] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 4622, A. Menezes, Ed. Berlin, Germany: Springer-Verlag, pp. 535–552, 2007.

[43] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart, "Deterministic encryption: Definitional equivalences and constructions without random oracles," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 5157, D. Wagner, Ed. Berlin, Germany: Springer-Verlag, pp. 360–378, 2008.

[44] A. Boldyreva, S. Fehr, and A. O'Neill, "On notions of security for deterministic encryption, and efficient constructions without random oracles," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 5157, D. Wagner, Ed. Berlin, Germany: Springer-Verlag, pp. 335–359, 2008.

[45] Z. Brakerski and G. Segev, "Better security for deterministic public-key encryption: The auxiliary-input setting," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 6841, P. Rogaway, Ed. Berlin, Germany: Springer-Verlag, pp. 543–560, 2011.

[46] J.W. Byun et al., "Offline Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data," Proc. Third VLDB Int'l Conf. Secure Data Management, pp. 75-83, 2006.

[47] I.R. Jeong et al., "Constructing PEKS Schemes Secure against Keyword Guessing Attacks Is Possible?," Computer Comm, vol. 32, no. 2, pp. 394-396, 2009.

[48] Liming Fang, Willy Susilo, Chunpeng Ge, Jiandong Wang, "A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle," CANS 2009, pp. 248-258, 2009.

[49] Qiang Tang, Liqun Chen, "Public-Key Encryption with Registered Keyword Search," EuroPKI 2009, pp. 163-178, 2009.

[50] W. Harrower, "Searching Encrypted Data," Technical report, Dept. of Computing, Imperial College London, 2009.

[51] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[52] Wei Wang, Peng Xu, Hui Li, Laurence Tianruo Yang, "Secure Hybrid-Indexed Search for High Efficiency over Keyword Searchable Ciphertexts," Future Generation Computer Systems, 55, pp. 353-361, Feb. 2016.

[53] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, "Generating Searchable Public-Key Ciphertexts With Hidden Structures for Fast Keyword Search" *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1667-1680, Sep. 2015.

[54] Peng Xu, Jingnan Li, Wei Wang, Hai Jin, "Anonymous Identity-Based Broadcast Encryption with Constant Decryption Complexity and Strong Security," ASIACCS 2016, pp. 223-233, 2016.

[55] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, pp. 247–267, 2007.

[56] K. Niu, X. A. Wang, and M. Zhang. "How to Solve Key Escrow-Problem in Proxy Re-encryption from CBE to IBE," In *Proceedings of DBTA 2009*, pages 95-98. IEEE, 2009

[57] X. A. Wang, X. Yang, and M. Zhang. "Proxy Re-encryption Scheme from IBE to CBE," In *Proceedings of DBTA 2009*, pages 99-102. IEEE, 2009.

[58] J. D. Zhang, X.A. Wang and X.Y. Yang. Hybrid proxy re-encryption between IBE and CBE. Journal of Computers, vol. 8, no. 7, pp 1873-1881, 2013.

[59] P. Wei, X.A. Wang and X.Y. Yang. Proxy Re-Encryption from CLE to CBE. in: Proceedings of International Conference on Computational Intelligence and Security, Nanning China, pp 339-342, 2010.

[60] T. Mizuno and H. Doi. Hybrid Proxy Re-encryption Scheme for Attribute-Based Encryption. in: Proceedings of 5th International Conference on Information Security and Cryptology, Beijing, China, pp 288~302, 2009.

[61] Q. Tang, P. H. Hartel, and W. Jonker. "Inter-domain Identity-Based Proxy Re-encryption," In *Proceedings of Inscrypt 2008*, LNCS, Vol. 5487, pages 332-347. Springer, 2009.

[62] P. Xu, H. Chen, D. Zou, and H. Jin. "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," *Chinese Science Bulletin,* 59(32): 4201-4209, 2014.

[63] P. Xu, J. Xu, W. Wang, H. Jin, W. Susilo, D. Zou, "Generally Hybrid Proxy Re-Encryption: A Secure Data Sharing among Cryptographic Clouds" in Proc. 11th ACM on Asia Conference on Computer and Communications Security, pp. 913-918, 2016.

徐鹏 于 2010 年在华中科技大学信息安全专业获得博士学位, 现任华中科技大学服务计算技术与系统教育部重点实验室副教授, 研究领域为密码学, 研究兴趣包括: 基于身份密码学、格密码学、可搜索加密、云安全、物联网安全等。Email: xupeng@hust.edu.cn

金海 于 1994 年在华中理工大学(现华中科技大学)计算机系统结构专业获得博士学位, 现任华中科技大学服务计算技术与系统教育部重点实验室主任、集群与网格计算湖北省重点实验室主任、大数据技术与系统湖北省工程实验室主任, 研究领域为计算机体系结构、计算系统虚拟化、云计算、云安全等。Email: hjin@hust.edu.cn

陈天阳 于 2017 年在华中科技大学信息安全专业获得学士学位, 现在华中科技大学信息安全专业攻读硕士研究生, 研究领域为密码学, 主要研究兴趣包括基于身份密码学、可搜索加密、云安全、物联网安全等。Email: chentianyang@hust.edu.cn