计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190323
56(10):2160-2169,2019

支持属性撤销的可追踪外包属性加密方案

高嘉昕　孙加萌　秦　静
(山东大学数学学院　济南　250100)
(gaojiaxin507@163.com)

Traceable Outsourcing Attribute-Based Encryption with Attribute Revocation

Gao Jiaxin, Sun Jiameng, and Qin Jing
(*School of Mathematics*, *Shandong University*, *Jinan* 250100)

Abstract　Attribute-based encryption (ABE) is a new type of public key encryption method that can implement fine-grained access control on data in cloud servers, but the computational overhead of key distribution, data encryption and data decryption processes in attribute-based encryption is too expensive, which causes a large computational burden on the user with limited computing resources. In order to solve this problem, this paper constructs an attribute-based encryption scheme which supports key attribute revocation, outsource key distribution and data decryption work to the cloud server, at the same time, the proposed scheme can verify the correctness of outsourcing computation by using Hash functions; the scheme uses online/offline encryption and transfers lots of computation to the offline, which can effectively protect the privacy of user data, reduce the amount of user computing, and promote the operation efficiency of the solution; in addition, we use the tree access policy to provide more fine-grained access control; and the method of re-encryption realizes fine-grained attribute revocation, revoking a single attribute indirectly by generating a re-encryption key to update attributes and ciphertext; Finally, the user identity is embedded into the key to achieve the user traceability property. The proposed scheme is proved to be indistinguishable against chosen-plaintext attack(IND-CPA) security under the standard model.

Key words　attribute-based encryption (ABE); outsourcing computation; attribute revocation; cloud storage; verifiability

摘　要　属性基加密是一种能够对云服务器中数据实现细粒度访问控制的新型公钥加密方法,但是属性基加密中密钥分配、数据加密和解密过程的计算开销过大,给资源受限的用户造成很大的计算负担.为解决该问题,构造了一个将密钥分配与解密工作外包给云服务器的支持属性撤销的属性加密方案,同时该方案可验证外包计算的正确性.该方案使用线上/线下加密,既有效保护用户数据的隐私性,又减少用户的计算开销,提升方案运行效率;其次方案中使用树形访问策略,以提供更加细粒度的访问控制;同时利用重加密的方法实现细粒度的属性撤销,通过生成重加密密钥更新属性与密文,间接撤销单个属性;最后将用户身份嵌入密钥,达到用户可追踪的性质,并在标准模型下证明该方案是选择明文的不可区分安全性.

收稿日期:2019-05-31;**修回日期**:2019-07-31
基金项目:国家自然科学基金项目(61772311)
This work was supported by the National Natural Science Foundation of China(61772311).
通信作者:秦静(qinjing@sdu.edu.com)

关键词 属性加密;外包计算;属性撤销;云存储;可验证性

中图法分类号 TP309.2

随着社会发展,数据呈现爆炸性增长,用户对计算机的存储和计算能力有了更高要求,由于资源和成本的限制,用户往往拥有有限的计算和存储能力,难以达到数据处理所需要的条件.在这种背景下,云服务器的概念就产生了.服务商平台陆续为用户提供云服务器来解决用户的资源受限问题,如华为云、阿里云、百度云等.信息上传到云服务器存储和加密,为用户带来便利的同时也出现了安全问题,即云服务器并不是完全可信的.用户的敏感信息上传到云服务器后,一方面信息脱离了用户的物理掌控,用户不能确保信息的隐私性和正确性;另一方面用户的敏感信息未经处理上传到云服务器,云服务器的管理者可以访问数据并窃取敏感信息,数据的隐私性遭到破坏.2011~2014 年间约有 11.4 亿人遭遇隐私数据被泄露的危机.2012 年苹果 ICloud 的访问控制出现问题,导致大量用户存储在 ICloud 的数据被盗,不仅给用户造成了巨大的损失,也给苹果公司的股价和形象带来了负面影响[1-2].随着技术的发展,访问控制在云计算中拥有越来越高的地位.而在云计算中,目前应用较为广泛的访问控制是基于属性加密技术.

基于属性的加密(attribute-based encryption,ABE)[3]是一种新型加密原语,在云计算中有着广泛的应用.在 ABE 体制中用户的私钥和密文分别用一组描述属性和访问策略标记,当描述的属性与访问策略相关联时,即私钥与密文相关联时才能正确解密.ABE 有 2 种形式:密钥策略 ABE(key-policy ABE,KP-ABE)和密文策略 ABE(ciphertext-policy ABE,CP-ABE).KP-ABE 是指密文由属性标记,私钥由访问策略标记.而在 CP-ABE 中私钥由属性标记,密文由访问策略标记,由数据发送方决定访问策略.ABE 体制中用户可以设置访问策略,并决定与访问策略相关联的属性,即哪些属性可以解开密文,因此用户对数据具有灵活的访问控制权.基于属性的加密技术可以在云服务器不完全可信的情况下,通过访问控制保障云服务器中的数据安全.但是属性加密中密钥分配和解密计算的巨大开销和存储量,使得计算能力不足的用户很难应用属性加密技术保障信息安全.

为了解决这个问题,Green 等人[4]和 Zhou 等人[5]提出在不泄露隐私数据和密钥的前提下将 ABE 体制中的解密阶段外包给云服务器计算.即将属性加密中计算成本大的部分外包给云服务器计算,解决了用户计算负担过重的问题,也加快了方案的运行效率.文中所构造的方案在不受信任的云服务器环境下,虽然减少了用户的计算和存储开销,但是用户无法对服务器返回的结果进行验证.2014 年 Li 等人[6]提出了引用计算委托(refered delegation of computation,RDoC)的模型,首先方案支持密钥委托生成,将部分密钥生成过程外包给 k 个服务器,在权限端进行验证并生成转化密钥,既加快了方案运行效率,又完善了部分外包计算的可验证性,解决了用户不能对返回结果验证的问题,这是第 1 次考虑部分外包 ABE 的可验证性;其次将部分解密工作外包给服务器计算,减少了用户的计算负担,通过盲化密钥保护解密密钥的安全性.但是该方案中数据消息未经处理直接发送给云服务器,不能有效保护数据的隐私性,同时也不支持属性撤销和可追踪性.

本文基于 Li 等人[6]的 ABE 方案构造了一个可验证的外包 KP-ABE 方案,本文方案使用具有高表达性的树形访问策略,提供了更细粒度的访问控制,丰富了属性之间的逻辑关系;将加密阶段分为线上、线下 2 部分进行,线下加密指将部分只需要公钥进行的计算转移至线下进行,既减少用户计算存储量,又有效保护用户数据的隐私性;面对不可避免的用户访问权限变更问题,本文通过重加密的方法生成重加密密钥更新属性与密文,间接撤销单个属性,达到细粒度属性撤销,实现用户的动态加入及退出;最后将用户身份嵌入到用户私钥中,通过泄露的密钥即可追踪到用户身份,有效解决了密钥的泄露问题,防止合谋攻击.

1 相关工作

1.1 基于属性的加密

ABE 体制最初由 Sahai 和 Waters[3]于 2005 年提出,正式提出了满足可容忍误差性和防止串谋攻击性的生物识别技术与基于属性加密技术.文中首次将身份与一组属性相关联,并正式给出了基于多项式插值的 ABE 具体构造方案.随后 2006 年 Goyal 等人[7]提出了由数据接收方规定访问策略的 KP-ABE,解决了基于属性加密技术无法支持灵活的访

问控制问题.2007 年 Bethencourt 等人[8]首次详细描述了 CP-ABE 方案以及 CP-ABE 的特性,文中所构造的 CP-ABE 方案的访问控制由更为灵活的树形访问结构描述,在典型的访问控制树中,非叶子节点为陷门,叶子节点为属性值.树形访问结构也是 ABE 方案中应用较为广泛的访问控制.

在实际应用中,ABE 系统也难免面临着用户权限的改变、用户的删除与更新等问题,在 2010 年 Yu 等人[9]提出了 CP-ABE 的属性撤销方案.在这篇文章中采用了半可信的代理服务器进行代理重加密技术,在撤销属性时只需生成重加密密钥即可,并在文中提出了 KP-ABE 的大属性空间撤销方案.但是 ABE 中关于访问结构中关联的一系列属性以及其他运算的高额运算量依旧没有得到解决,Hohenberger 和 Waters 在 2014 年提出了线上/线下 ABE[10],通过将部分计算转移到线下减少线上的计算量,有效地提高计算效率,减少用户的计算量.

随着互联网的快速发展,移动终端与云存储的结合成为未来趋势,但是移动终端的计算资源受限,传统的属性加密技术往往需要大量的计算,给属性授权机构和移动终端带来严重的计算负担,相关学者提出将外包计算与属性加密技术相结合达到减少用户计算负担的目的.2017 年,Zhao 等人[11]提出了面向移动云计算的外包 ABE 方案.该方案支持加密外包和解密外包,解决了基于属性加密的高效性带来的解密计算中的高额计算量.Fan 等人[12]提出了一种多授权中心的可验外包计算.Zhang 等人[13]提出一种完全外包 ABE 方案,即将密钥生成、加密和解密都外包给云服务商,并且完成了方案的安全性证明.但该方案无法完成外包计算正确性的验证,而可验证性对于正确计算至关重要.Li 等人[14]提出一种新的可验证外包解密计算,该方案只实现了解密外包,而数据拥有者仍然需要大量计算完成数据加密任务.2014 年 Li 等人[6]提出了一个同时支持密钥生成和解密外包的属性加密方案,将密钥生成和部分解密工作外包给不同的服务器计算,使得资源受限的用户也可以进行计算繁重的任务.该方案不仅减轻了用户的计算负担,也对返回结果的正确性进行验证,但是方案中用户上传到云服务器的数据隐私性等问题仍没有解决.

2019 年 Zhao 等人[15]提出一种可验证的完全外包的 CP-ABE 方案,即将密钥产生、加密和解密都外包给云服务商,并完善了完全外包方案的可验证性,并且给出了该方案的选择明文攻击下的不可区分性安全和可验证安全性证明.

1.2 外包计算

外包计算是一项新兴技术,它有效地解决了计算能力及存储空间不足等问题.Chaum 等人[16]在 1995 年提出了外包密码运算的雏形,即通过在用户的设备上安装安全的硬件来帮助用户完成复杂的计算.随后在 2005 年 Hohenberger 等人[17]给出外包计算的安全定义,并且提出了一个全新的外包计算方案,文中具体算法是基于模指数运算提出的.2010 年 Gennaro 等人[18]首次提出了非交互式可验证计算的概念,并且基于混淆电路和全同态加密提出一个适用于任意运算的可验证的外包计算,将待计算的函数转化成相对的电路函数.2011 年 Green 等人[4]给出了支持解密运算外包的基于属性加密方案,但是方案没有考虑到用户对于返回结果的验证问题.随后 Lai 等人[19]通过增加密文冗余的方法改善了之前不支持外包计算结果的正确性验证.

Dong 等人[20]提出了基于双线性对的完全可验证安全外包.2014 年 Li 等人[6]提出了一个同时支持密钥生成和解密外包的属性加密方案,既能达到将计算外包的目的,也可以对返回结果的正确性进行验证.随后出现了大量以数学运算为基础的安全外包,2015 年 Chen 等人[21]利用稀疏矩阵提出一个安全的矩阵外包方案.2016 年 Yu 等人[22]对大规模线性方程组求解的安全外包进行了深入研究,2017 年 Kumar 等人[23]提出了对于恶意的云服务器如何利用矩阵乘法安全外包.

1.3 线上/线下技术

线上/线下技术是一种可以有效提高加密效率和签名效率的密码学工具,它将加密和签名过程分为线上和线下 2 个部分进行,在线下对加密或签名的高计算量部分进行预处理,使得轻量级设备只需进行少量计算即可得到密文和签名,有效地解决了资源受限的用户计算量不足的问题.

最初在 1989 年 Even 等人[24]提出了线上/线下签名的概念,作者在线下进行签名的高计算率部分,将轻量级的计算在线上进行,虽然有效减少了计算量,但是增加了签名的长度.随后,2001 年 Shamir 等人[25]提出了一个更高效的线上/线下签名方案,所提出的线上/线下签名无需将签名的长度增加一个二次因子.

2008 年 Guo 等人[26]正式提出基于身份的线上/线下加密方案,在这个方案中将加密过程分成线上加密和线下加密 2 个部分,线下完成大部分加密计算,但不知道消息与接收方的身份,保存部分密

文,线上只需要进行少量的加密计算即可得到密文.线上/线下加密既有效保护信息安全性,又减少存储空间和计算成本的浪费.

2 预备知识

2.1 符 号

本文所用到的缩略词如表 1 所示:

Table 1 Related Terms and Their Acronyms

表 1 相关名词及缩略语

Acronym	Description
DO	Data Owner
DU	Data User
SK	Secret Key
PK	Public Key
AA	Attribute Authority
KGSP	Key Generation Service Provider
DSP	Decryption Service Provider
SSP	Storage Service Provider
OK	Outsourcing Key
TK	Transformation Key

其中,本文中属性机构 AA 是可信任的,但密钥生成服务商 KGSP、云存储服务商 SSP 和解密服务商 DSP 是"诚实且好奇"(honest but curious)的,即云服务器会遵守协议,但是会试图获取更多的隐私信息.

2.2 相关定义

定义 1. 访问结构.设$\{P_1,P_2,\cdots,P_n\}$为 n 个参与者的集合,如果$\forall B,C$ 满足$B\in A,B\subseteq C$,则$C\in A$,集合$A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$是单调的.其中属于 A 的集合称为认证集.此外本文定义 $\gamma(\cdot,\cdot)$,

$$\gamma(\omega,A)=\begin{cases}1, & \omega\in A,\\ 0, & \text{其他}.\end{cases}$$

定义 2. 访问树.在一棵访问树中,其根节点为 r,所有的叶子节点 m 均为输入的属性值,每一个节点关联一个 d_m 阶多项式 $q_m(\cdot)$,其中 $d_m=k_m-1$,k_m 为该节点的门限值.所有的非叶子结点 m 则是门限值为 k_m 的陷门,其中非叶子节点 m 拥有 num_m 个孩子节点.在访问树中,定义操作:

$parent(m)$表示节点 m 的父节点,$children(m)$表示节点 m 的子节点,$index(m)$表示兄弟节点中的序号,$att(m)$表示叶子节点所关联的属性.

定义 3. 双线性映射.设置 2 个阶为素数 q 的乘法循环群 G 和 G_T,g 是 G 的一个生成元.存在一个双线性映射 $e:G\times G\mapsto G_T$,满足 3 个属性:

1) 双线性.$\forall g_1,g_2\in G$,$\forall a,b\in_R Z_q$ 都有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$.

2) 非退化性.$\exists g_1,g_2\in G$ 满足 $e(g_1,g_2)\neq 1$.

3) 可计算性.$\forall g_1,g_2\in G$,计算 $e(g_1,g_2)$是有效函数.

2.3 困难假设

定义 4. 判定双线性 Diffie-Hellman 问题(decision bilinear Diffie-Hellman problem, DBDH).假设给定一个四元组(g,g^a,g^b,g^c),其中 g 是阶为 q 的乘法循环群 G 的生成元,$a,b,c,z\in Z_q$,区分 2 个四元组$(g^a,g^b,g^c,e(g,g)^{abc})$和$(g^a,g^b,g^c,e(g,g)^z)$.如果对于多项式时间内解决 DBDH 的概率是可以忽略的,就说 DBDH 问题是困难的.

3 模型定义

3.1 VDC-KP-ABE 方案模型

图 1 给出本文所提 VDC-KP-ABE(delegation of computation KP-ABE with verifiability)方案模型.

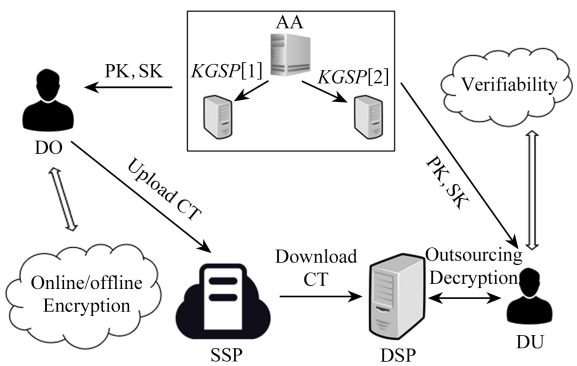

Fig.1 System model for this paper

图 1 本文方案的模型

用户向 AA 请求密钥,AA 将密钥生成阶段外包给 $KGSP[i]$进行,对返回结果进行检验后将密钥发送给用户.用户将密文发送到 SSP 存储,解密过程中,用户从 SSP 中搜索下载密文,并将解密工作外包给 DSP 进行,用户可以对返回结果进行验证.

在密钥分配过程中,为了防止 KGSP 与 DSP 串通下的不诚实行为,利用 AA 生成的 $d-1$ 阶随机多项式 $g_{RG}(\cdot)$,将 $g_{RG}(\cdot)$与另一个多项式以随机的顺序发送给 $KGSP[i]$.KGSP 利用多项式生成部分转化密钥,AA 只需要检验由 $g_{RG}(\cdot)$计算的部分转化密钥即可.

记 A 为访问策略,ω 为属性集合.

根据系统模型,算法定义:

1) 初始化算法

$Setup(\lambda)\rightarrow(PK,MK)$:AA 运行该算法,输入为系统的安全参数 λ.输出为公钥 PK 和主密钥 MK.

2) 密钥生成

$KeyGen_{\text{init}}(A,MK,ID)\rightarrow(S[i]_{\text{REAL}},S_{\text{RG}})$:AA 运行密钥生成初始化算法,输入属性访问策略 A 和主密钥 MK,输出一对外包密钥集($OK_{KGSP[i]}$,OK_{AA})和一组基于外包密钥 $OK_{KGSP[i]}$ 生成的数对 $(S[i]_{\text{REAL}},S_{\text{RG}})$.

$KeyGen_{\text{out}}(S[i]_{\text{REAL}},S_{\text{RG}})\rightarrow(TK_{KGSP[i]},TK_{RG_i})$:$KGSP[i]$被委托计算部分转化密钥,即运行密钥生成算法.算法中的输入为$(S[i]_{\text{REAL}},S_{\text{RG}})$,最终输出部分转化密钥对$(TK_{KGSP[i]},TK_{RG_i})$.

$KeyGen_{\text{in}}(A,OK_{\text{AA}})\rightarrow TK_{\text{AA}}$:由 AA 运行内部密钥生成算法,输入为树形访问策略 A 和 AA 的外包密钥 OK_{AA},输出另一个部分转化密钥 TK_{AA}.

$KeyCheck(TK_{KGSP[i]},TK_{RG_i},ID)\rightarrow TK$:AA 对 KGSP 发回的结果进行检验,通过验证后输出转化密钥 TK.

$KeyBlind(TK)\rightarrow(SK,TK')$:由 AA 计算,输入转化密钥 TK,输出私钥 SK 和盲化密钥 TK'.

3) 加密算法

$Encrypt_{\text{off}}(PK)\rightarrow CT_{\text{off}}$:线下执行加密算法,输入公钥 PK,输出部分密文 CT_{off}.

$Encrypt_U(M,CT_{\text{off}},\gamma)\rightarrow(CT,VK)$:用户进行加密计算,输入消息 M、加密属性 γ 和部分密文 CT_{off},输出密文 CT 和验证密钥 VK.

4) 解密算法

$Decrypt_{\text{out}}(CT,TK')\rightarrow CT_{\text{part}}$:DSP 执行算法,输入与属性集相关的密文 CT 和包含访问策略 A 的转化密钥 TK',输出部分解密密文 CT_{part}.

$Decrypt_{\text{in}}(CT_{\text{part}},SK,VK)\rightarrow M/\perp$:用户执行最后解密算法,输入部分解密密文 CT_{part}、私钥 SK 和验证密钥 VK,首先对 DSP 返回结果进行验证,若通过验证,输出明文 M,否则输出 $\perp$.

5) 属性撤销

$ReKeyGen(\theta,MK)\rightarrow rk$:由 AA 计算,输入更新的属性集 θ,和主密钥 MK 生成重加密密钥 rk.

$ReEnc(E,rk,\beta)\rightarrow CT'$:输入属性集 β、密文 CT 和重加密密钥 rk,输出更新后的密文 CT'.

$ReKey(SK,rk)\rightarrow SK'$:输入密钥 SK 和重加密密钥 rk,输出更新后的密钥 SK'.

6) 追踪算法

$Trace(SK)\rightarrow ID$:输入密钥 SK,对密钥进行验证是否为正常,如果通过验证,则可以得知密钥所属用户的 ID.

3.2 安全模型

1) 选择安全性游戏

考虑未授权和授权已撤销 2 种攻击者,重加密密文与原始密文分布相同,因此只讨论原始密文的安全性.本文针对所提出的 VDC-KP-ABE 方案描述攻击者 A 与挑战者 B 之间的游戏如下:

初始化.攻击者 A 选择要挑战的一个属性集合和撤销的属性列表发送给挑战者 B.

系统建立.挑战者 B 运行本文方案的 $Setup$ 阶段,将公钥发送给攻击者.

询问阶段 1.攻击者可以询问关于访问策略属性的私钥,其中属性不属于访问策略,或者属性属于撤销属性列表中.

挑战:挑战者对于攻击者发送的消息 M_0,M_1,挑战者随机投掷一枚硬币 $v\in\{0,1\}$,在属性集和撤销的属性列表下对 M_v 进行加密,并将结果返回给攻击者 A.

询问阶段 2.重复询问阶段 1 的步骤.

猜测.攻击者输出对 v 的猜测 v',若 $v'=v$,则攻击者赢得游戏.

定义 5. IND-CPA 安全.若多项式时间攻击者以可忽略的优势攻破上述安全模型,那么我们就说本文提出的方案是 IND-CPA 安全的.其中,攻击者的优势为 $Adv=\left|Pr[v'=v]-\frac{1}{2}\right|$.

2) 可验证性游戏

可验证性可以验证外包阶段的算法是否有被正确执行.通过攻击者 A 与挑战者 B 之间的交互描述 VDC-KP-ABE 方案的可验证性.

初始化.攻击者 A 选择要挑战的 2 个 Hash 函数.

系统建立.挑战者 B 运行本文方案的 $Setup$ 阶段,将公钥发送给攻击者,自己保留主私钥.

询问阶段 1.挑战者 B 按照方案算法生成方式适应性回答攻击者 A 的询问

挑战.攻击者 A 提交一个密文 M^* 和一个访问策略 A^*,挑战者 B 运行 Enc 算法获得密文 CT^* 和验证密钥 VK^*.

询问阶段 2.重复询问阶段 1 的步骤,但是攻击者不可以询问属于访问策略 A^* 的属性.

猜测阶段.A 输出转换密文 CT^*_{part}.若 $Decrypt_{\text{in}}$

$(CT^*_{\text{part}}, RK^*, VK^*) \notin (m^*, \perp)$,则攻击者 A 赢得了游戏.

定义 6. 可验证性安全.若无多项式时间攻击者以不可忽略的优势攻破上述安全模型,那么我们就说本文提出的方案具有可验证性.

4 本文方案

在密钥委托生成过程,本文利用一个混合密钥策略 $Policy = Policy_{\text{KGSP}} \wedge Policy_{\text{AA}}$,其中 $\wedge$ 是连接 2 个子策略的和门,$Policy_{\text{KGSP}}$ 是用于用户请求的属性集,$Policy_{\text{AA}}$ 是用于一个“不重要”的属性.称之为“不重要”属性的原因是每个请求的属性集都附加一个对整个访问控制策略没有影响的“不重要”属性 θ.利用这个技巧可以随机生成一个外包密钥 OK_{KGSP},无需主密钥和私钥的前提下,将密钥生成阶段外包给 KGSP 进行.

4.1 VDC-KP-ABE 方案构造

1) 初始化算法

$Setup(1^\lambda)$:定义属性全集 U 和身份全集 I.首先,将全集 U 和 I 中的属性定义为 Z_q 中的元素.简单起见取 Z_q 中前 n 个元素为全集.定义 Hash 函数 $H:\{0,1\}^* \to Z_p$,$H_0:\{0,1\}^* \to \{0,1\}^\lambda$,$H_1:\{0,1\}^{2\lambda} \to \{0,1\}^*$.选择一个生成元 $g \in_R G$,整数 $x, a, w, w_1, w_2, \cdots, w_n \in_R Z_q$,并设 $g_1 = g^x$,$W = g^w$,$W_i = g^{w_i}$,选择元素 $g_2 \in_R G$.最终输出公钥 $PK = (g, g_1, g_2, W, W_1, \cdots, W_n, H, H_0, H_1)$ 和主私钥 $MK = (x, a, w, w_1, \cdots, w_n)$.

2) 密钥生成

$KeyGen_{\text{init}}$:AA 选择 $x_{11}, x_{12} \in_R Z_q$,并设 $OK_{\text{AA}} = x_2 = x - x_{11} - x_{12} \bmod q$.接下来随机选取 d_m 阶多项式 $f_m(\cdot)$,$p_m(\cdot)$.满足:

① $i = att(m)$ 时,$f_m(i) = p_m(i)$;

② $f_m(0) = x_{11}$;

③ $p_m(0) = x_{12}$;

④ $f_m(i) + p_m(i) = q_m(i)$,其中 $i = att(m)$,$att(m)$ 表示叶子节点所关联的属性.

选择一个随机多项式 $g_{\text{RG}}(\cdot)$.此外,选取 $r_{KGSP[1],i}$,$r_{KGSP[2],i}$,$r_{RG,i} \in Z_p$,满足 $r_{KGSP[1],i} = r_{KGSP[2],i}$,$r_i = r_{KGSP[1],i} + r_{KGSP[2],i}$,$i = att(m)$.最后,AA 将 $(S[1]_{\text{REAL}}, S_{\text{RG}})$,$(S[2]_{\text{REAL}}, S_{\text{RG}})$ 分别发送给 $KGSP[1]$,$KGSP[2]$.其中:

$$S[1]_{\text{REAL}} = (f_m(0)H(ID), \{r_{KGSP[1],i}\}_{i=att(m)}),$$

$$S[2]_{\text{REAL}} = (p_m(0)H(ID), \{r_{KGSP[2],i}\}_{i=att(m)}),$$

$$S_{\text{RG}} = (g_{\text{RG}}(\cdot), \{r_{RG,i}\}_{i=att(m)}).$$

$KeyGen_{\text{out}}$:$KGSP[j]$ 计算部分转化密钥,即 $TK_{KGSP[j]} = (\{d[j]_{i0}, d[j]_{i1}\}_{i=att(m)})$ 和 $TK_{RG_j} = (\{d[RG_j]_{i0}, d[RG_j]_{i1}\})$,并将 $(TK_{KGSP[j]}, TK_{RG_j})$ 发送给 AA.其中:

$$d[1]_{i0} = g_2^{f_m(0)H(ID)}(g_1 h_i)^{r_{KGSP[1],i}},$$

$$d[2]_{i0} = g_2^{p_m(0)H(ID)}(g_1 h_i)^{r_{KGSP[2],i}},$$

$$d[j]_{i1} = g^{r_{KGSP[j],i}},$$

$$d[RG_j]_{i0} = g_2^{q_{RG}(i)}(g_1 h_i)^{r_{RG,i}},$$

$$d[RG_j]_{i1} = g^{r_{RG,i}}, i = att(m), j = 1, 2.$$

$KeyGen_{\text{in}}$:AA 随机选择 $r_\theta \in_R Z_q$,并计算 $d_{\theta 0} = g_2^{x_2 H(ID)} \times (g_1 h)^{r_\theta}$,$d_{\theta 1} = g^{r_\theta}$.最后输出 $TK_{\text{AA}} = (\{d_{\theta 0}, d_{\theta 1}\})$.

$KeyCheck$:AA 检查所有的 KGSP 都是正确的输出,也就是检验

$$d[1]_{i0} = d[2]_{i0}, d[1]_{i1} = d[2]_{i1};$$

$$d[RG_1]_{i0} = d[RG_2]_{i0}, d[RG_1]_{i1} = d[RG_2]_{i1};$$

其中,$i = att(m)$.

通过计算 $d_{i0} = d[1]_{i0} \cdot d[2]_{i0}$,$d_{i1} = d[1]_{i1} \times d[2]_{i1}$,$i = att(x)$ 将部分转化密钥合并,并输出转化密钥 $TK = (\{d_{i0}, d_{i1}\}_{i \in A \cup \theta})$.

$Keyblind$:首先随机选取 $t \in_R Z_q$,令 $RK = t$,计算转化密钥 $TK' = (\{d'^t_{i0}, d'^t_{i1}\}_{i \in A \cup \theta})$,然后计算 $D_0 = g_2^{x + aH(ID)}$,$D_1 = g_1^{aH(ID)}$,$D_2 = ID$,最后可以得到用户私钥为 $SK = (t, TK', D_0, D_1, D_2)$.

3) 加密算法

$Encrypt_{\text{off}}$:选择一个随机数 $s \in_R Z_q$,然后计算 $K = e(g_1, g_2)^s$,$C_0 = g^s$,$C_i = (g_1 W_i)^s$,生成部分密文 $CT_{\text{off}} = (K, C_0, \{C_i\}_{i \in U})$.

$Encrypt_U$:用户在明文后附加一串冗余,即 $M_T = M \| 0^k$,用来在解密后检验 DSP 是否有不诚实行为;计算 $C_1 = M_T \times K^{H(ID)}$,$VK = H_1(H_0(K^{H(ID)}) \| C_1)$,生成密文 $CT_S = (\gamma \cup \theta, C_1, C_0, \{C_i\}_{i \in \gamma \cup \{\theta\}})$ 和验证标志.

4) 解密算法

$Dncrypt_{\text{out}}$:首先定义一个递归算法 $DecryNode(E, D, m)$,记 $i = att(m)$.

① 若 m 是叶子节点,则:

$$DecryNode(E, D, m) = \begin{cases} \dfrac{e(g^s, g_2^{tH(ID)(f_m(0)+p_m(0))}(g_1 W_i)^{tr_i})}{e(g^{tr_i}, (g_1 W_i)^s)} = \\ e(g, g_2)^{stH(ID) \times q_m(0)}, i \in \gamma, \\ \perp, \text{其他}. \end{cases}$$

② 若 m 非叶子节点,那么对于 m 的任意孩子

节点 z 调用递归算法 $DecryNode(E,D,m)$,并将输出记为 F_z.S_m 是任意 num_m 个子节点的集合,则:

$$F_m=\prod_{z\in S_x}F_z^{\Delta_{i,S_m}}=$$
$$\prod_{z\in S_m}(e(g,g_2)^{stH(ID)\times q_z(0)})^{\Delta_{i,S_m}(0)}=$$
$$\prod_{z\in S_m}(e(g,g_2)^{stH(ID)\times q_{parent(z)}(index(z))})^{\Delta_{i,S_m}(0)}=$$
$$\prod_{z\in S_m}(e(g,g_2)^{stH(ID)\times q_m(i)})^{\Delta_{i,S_m}(0)}=$$
$$e(g,g_2)^{stH(ID)\times q_m(0)}.$$

若密文满足访问策略树,则该递归算法将返回计算结果:

$$B=\frac{e(C_0,d_{\theta 0}^t)}{e(d_{\theta 1}^t,W_\theta)}DecryptNode(E,D,r)=$$
$$e(g,g_2)^{xtsH(ID)}=e(g_1,g_2)^{tsH(ID)}.$$

$Dncrypt_U$:用户收到 B 后,计算 $R=(B)^{\frac{1}{t}}=e(g_1,g_2)^{sH(ID)}$,若 $H_1(H_0(R)\|C_1)\neq VK$,则输出终止符⊥;否则计算

$$\frac{C_1}{(B)^{\frac{1}{t}}}=\frac{M_T\times e(g_1,g_3)^s}{e(g_1,g_2)^{sH(ID)}}=M_T.$$

用户检查是否附有一个冗余 0^k.如果是,则可以得到 M;否则 DSP 则存在不诚实的行为,输出终止符⊥.

5) 属性撤销

$ReKeyGen$:θ 为待更新的属性集,对于所有属性元素 $X\in\theta$,计算重加密密钥 $rk_X=\frac{x+t'_X}{x+t_X}$.待更新的属性集中所有属性都采用上述方法进行转换.

$ReEnc$:对密文 CT 只需要更新 E_i 部分,因此对于所有 $X\in\beta$,有 $E_i=[(g_1g^{t_i})^s]^{rk_i}=(g_1g^{t'_i})^s=E'_i$.

$ReKey$:更新用户的部分私钥,保证未被撤销的用户仍可以对更新后的密文进行解密,$d_{i1}=(g^{r_i})^{rk_i^{-1}}=(g^{r_i})^{\frac{x+t_i}{x+t'_i}}$.

6) 追踪算法

验证用户身份密钥是否满足 $e(D_0,g)=e(D_1,g)e(g_1,g)$,当通过密钥检查时,可直接通过 D_2 查询拥有密钥的用户身份.

4.2 分 析

4.2.1 安全性分析

4.2.1.1 选择性安全

定理 1. 在 DBDH 的假设下本文所构造的 VDC-KP-ABE 方案具有不可区分选择明文攻击(indistinguishable chosen-plaintext attack, IND-CPA)安全.

证明. 若攻击者可以在一个概率多项式时间内以不可忽略的优势 ε 在 IND-CPA 安全模型下攻破本文方案,那我们就能创建一个挑战者 B 能够以不可忽略的优势解决 DBDH 问题.因此在分析中我们主要的任务是提供一个挑战者和攻击者之间的真实方案的正确模拟.

假设挑战者随机翻转一个二进制硬币 μ.当 $\mu=0$ 时,四元组为 $(X=g^x,Y=g^y,Z=g^z,T=e(g,g)^{xyz})$;否则,四元组为 $(X=g^x,Y=g^y,Z=g^z,T=e(g,g)^v)$.其中 $x,y,z,v\in Z_q$,挑战者 B 输出 μ' 作为 μ 的猜测值.

1) 初始化

挑战者 B 运行身份为 ID 的攻击者 A,并且接受挑战属性集 ω 和撤销列表 R.

2) 系统建立

挑战者 B 分配公钥如下:令 $g_1=X,g_2=Y$,$g_3=g_2^{H(ID)}$,$h=g_1^{-1}g^{-\alpha}$,其中 $\alpha\in_R Z_q$,$i\in\theta$ 时,$h_i=g_1^{-1}g^{\alpha_i}$,其中 $\alpha_i\in_R Z_q$;$i\notin\theta$ 时,$W_i=g^{\alpha_i}$,$\alpha_i\in_R Z_q$.挑战者 B 将公钥 $PK=(g,g_1,g_2,W,W_1,W_2,\cdots,W_n,H,H_0,H_1)$ 发送给攻击者 A.

3) 查询阶段 1

挑战者 B 初始化一个整数 $j=0$,一个空白的表 T,攻击者 A 询问访问结构 T.首先要确认访问结构节点对应的多项式,挑战者 B 随机选取 $x_2,x_{1b}\in_R Z_q$ 和 k_x 阶多项式 $f_x^{(b)}$,使得多项式满足 $f_x^{(b)}(0)=x_{1b}$.随机选取 $r_{KGSP[b]},r_\theta\in_R Z_q$,挑战者 B 计算

$$TK_{KGSP[b]}=(\{g_2^{f_X^{(b)}(0)H(ID)}(g_1h_i)^{rKGSP[b],i},$$
$$g^{rKGSP[b],i}\}_{i\in U-R}),$$
$$TK_{AA}=(g_2^{x_2H(ID)}(g_1h)^{r_\theta},g^{r_\theta}).$$

挑战者 B 设置

$$r_{KGSP[1-b],i}=-y\Delta_{j,S}(0)+r'_i,$$
$$TK_{KGSP[1-b]}=(\{d[1-b]_{i0},d[1-b]_{i1}\}_{i\in U-R}),$$

其中 $r'_i\in_R Z_q$:

① 当询问的属性满足访问结构,但询问的属性属于撤销列表时,

$$d[1-b]_{i0}=g_2^{\tau_i}(g_1h_i)^{rKGSP[1-b],i},$$
$$d[1-b]_{i1}=g^{rKGSP[1-b],i},$$

其中 $\tau_i=f_x^{(b)}(0)H(ID)$,$r_{KGSP[1-b],i}=r_{KGSP[b],i}$.

② 不满足访问结构时,

$$d[1-b]_{i0}=$$
$$g_2^{H(ID)\sum_{j\in I'}\Delta_{j,S(i)}\tau_j-(x_2+x_{1b}+\alpha_i)\Delta_{j,S(0)}}(g_1h_i)^{r'_i},$$
$$d[1-b]_{i1}=g^{-y\Delta_{j,S(0)}+r'_i}.$$

此外,$d_{i0}=d[b]_{i0}\times d[1-b]_{i0}$,$d_{i1}=d[b]_{i1}\times d[1-b]_{i1}$,其中 $i\in U$,挑战者 B 将计算 $TK=(\{d_{i0},d_{i1}\}_{i\in(U-R)\cup\theta})$,并设置 $j=j+1$,将$(j,\omega,\cdot,x_{1b},x_{1(1-b)},\cdot)$加入 T 后,返回 x_{1b}.

挑战者 B 验证$(i,\omega,\cdot,x_{1b},x_{1(1-b)},\cdot)$是否存在 T 中,若存在,则计算 $t=\frac{t'}{y}$,其中 $t'\in_R Z_q$,返回 $TK'=\{(d_{i0}^t,d_{i1}^t)_{i\in(U-R)\cup\theta}\}$;否则返回终止符$\perp$.

挑战者 B 验证$(i,\omega,\cdot,x_{1b},x_{1(1-b)},\cdot)$是否存在 T 中,若存在,则返回私钥 SK;否则返回终止符$\perp$.

4) 挑战

攻击者 A 向挑战者 B 提交 2 个明文 M_0,M_1. 挑战者 B 随机投掷硬币 v,选择随机数 $r\in_R Z_P$,并返回明文 M_v 加密后的结果,密文被模拟为

$$CT^*=(\omega\cup\theta,rM_vT^{H(ID)},g^z,g^{-za},\{g^{zai}\}_{i\in\omega\cup\theta}).$$

注意:

① 如果 $\mu=0$,则 $T=e(g,g)^{xyz}$.如果 $s=z$,则:

$$C_0=rM_vT=rM_ve(g,g)^{xyzH(ID)}=rM_ve(g_1,g_2)^{zH(ID)},$$

$$C_1=g^z,$$

$$E_\theta=g^{-za}=(g_1g_1^{-1}g^{-a})^z=(g_1h)^z,$$

$$E_i=g^{zai}=(g_1g_1^{-1}g^{ai})^z=(g_1h_i)^z,$$

其中,$i\in\omega\cup\theta$.

② 如果 $\mu=1$,则 $T=e(g,g)^v$,那么 $C_0=rM_ve(g,g)^v$.因为 v 是随机的,在攻击者 A 的视图里 C_0 也是随机的,因此加密后的消息不包含 M_v 的任何信息.

5) 查询阶段 2

重复查询阶段 1.

6) 猜测

攻击者 A 提供一个 v 的猜想 v'.如果 $v'=v$,挑战者 B 会输出 $\mu'=0$ 表示它是一个 DBDH 四元组.否则,它是一个随机四元组.

当 $\mu=1$ 时,攻击者 A 没有得到关于 v 的任何有用信息.因此我们可以得到 $Pr[v\neq v'|\mu=1]=\frac{1}{2}$.因为当 $v=v'$ 时,挑战者 B 猜测 $\mu'=1$,则 $Pr[\mu\neq\mu'|\mu=1]=\frac{1}{2}$.当 $\mu=0$ 时,攻击者 A 可以得到 M_v 的有效密文,在这个情形下,攻击者拥有优势 ε.因此我们可以得到 $Pr[v=v'|\mu=0]=\frac{1}{2}+\varepsilon$.因为当 $v=v'$时,挑战者 B 猜测 $\mu'=0$,则 $Pr[\mu=\mu'|\mu=0]=\frac{1}{2}+\varepsilon$.因此挑战者 B 赢得 DBDH 游戏的整体优势是:

$$\frac{1}{2}Pr[\mu=\mu'|\mu=0]+\frac{1}{2}Pr[\mu=\mu'|\mu=1]=\frac{1}{2}\varepsilon.$$

若攻击者在一个概率多项式时间赢得游戏的优势为 ε,则可以以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DBDH 困难问题.在安全模型中,攻击者存在不可忽略的优势 ε 才能打破本文方案.因此,本文方案是 IND-CPA 安全的. 证毕.

4.2.1.2 可验证性安全

定理 2. 假设 H_0 和 H_1 抵抗合谋攻击的 Hash 函数,那么 VDC-KP-ABE 方案具有可验证性.

证明.

假设:若攻击者 A 可以攻破本文方案的可验证性,那我们就能创建一个挑战者 B 能够以不可忽略的优势攻破 Hash 函数的抵抗合谋攻击特性.

初始化:攻击者提交 2 个 Hash 函数(H_0^*,H_1^*).

系统建立:挑战者执行 *Setup* 阶段,然后用(H_0^*,H_1^*)替换公钥中的(H_0,H_1).

阶段 1:B 按照方案算法生成方式适应性回答攻击者 A 的询问.

挑战阶段:攻击者 A 提交一个密文 M^* 和一个访问策略 A^*,挑战者运行 Enc 算法获得密文 CT^* 和验证 VK^*.

阶段 2:B 按照方案算法生成方式适应性回答攻击者 A 的询问,攻击者不可以询问属于访问策略 A^* 的属性.

猜测阶段:攻击者 A 输出转换密文 $CT^*_{\text{part}}=(C_1,B)$.

若攻击者 A 攻破可验证性,则挑战者 B 可以从 $Decrypt_{\text{in}}(CT^*_{\text{part}},RK^*,VK^*)$恢复出明文.

计算攻击者 A 成功的概率,只需考虑 2 种情况:

① $(H_0(R),C_1)\neq(H_0(R)^*,C_1^*)$,因为 B 知道 $(H_0(R)^*,C_1^*)$,则 B 得到 Hash 函数 H_1^* 的碰撞值.

② $(H_0(R),C_1)=(H_0(R)^*,C_1^*)$,但 $R\neq R^*$,因为 $H_0^*(R)\neq H_0^*(R^*)$,则 H_0^* 抗合谋性将被攻破.

综上所述,完成定理 2 的证明. 证毕.

4.2.2 效率

本节从理论上分析密钥生成、加密过程和解密过程的计算开销,将本文构造方案与文献[3,6,13]中方案进行计算效率对比.其中,E 表示 G 中指数计

算,P 表示对计算,M 表示群乘法计算.另外 W 表示属性集的大小,d 表示陷门值,l 表示线性秘密共享(LSSS)中生成矩阵的行数.指数、群乘法运算和双线性对的计算量相对于其他计算需要更多的计算时间,因此本文忽略了次要因素.

本文方案和文献[3,6,13]中方案的效率对比如表 2 所示.文献[3]中是原始 ABE 方案,与文献[3]中方案对比,本文方案将密钥分配和解密工作外包,并且可验证外包结果正确性,同时用户计算量减少,缓解了资源受限用户的计算负担问题,加快了方案运行效率,且支持属性撤销与用户追踪.与文献[13]方案相比,本文方案支持外包计算的可验证性,且计算效率更高.与文献[6]中 ABE 方案相比,本文构造的方案使用线下加密,既减少线上加密时间、加快方案效率,又有效保护用户数据的安全性,同时支持属性撤销和用户可追踪.

Table 2 Comparison of Efficiency

表 2 效率比较

Schemes	Key Generation		Encryption		Decryption		Revocation	Verifiability
	KGSP	AA	ESP	DO(on line)	DSP	DU		
Ref [3]		$2W$E		$(W+2)$M+E+P		$2d$P+$2d$E	×	×
Ref [13]	$(4W+3)$E	0	$(5l+1)$E	E	$(2d+2)$E+dE+$(3d+2)$P	E	×	×
Ref [6]	$2W$E	2E	$(W+2)$M+E+P	M	$2d$P+$2d$E	E	×	√
Ours	$2W$E	2E		M	$2W$P+$2W$E	E	√	√

Note: The tick indicates that this function is supported in the article, and the cross indicates that this function is not supported in the article.

5 总 结

为了满足计算、存储能力不足用户的访问需求,本文构造了将密钥分配和解密过程外包的属性加密方案,并且能够验证外包计算的正确性.该方案支持属性撤销,并且可追踪泄露密钥的用户.本文方案应用树形访问策略,达到更细粒度的访问控制;其次方案将加密过程分为在线阶段和离线阶段,离线阶段利用已知的公钥进行部分加密,既有效保护用户数据的隐私性,又减轻了用户的计算负担;针对实际应用中用户访问权限的变更,本文方案通过使用重加密的方法更新密文与密钥,支持基于访问树的细粒度属性撤销,并将用户身份嵌入到用户密钥中,既防止合谋攻击,又可以通过密钥追踪到用户身份.最后,在标准模型下基于 DBDH 假设证明了本文方案是 IND-CPA 安全的.

参 考 文 献

[1] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
(冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83)

[2] Park J, Sandhu R S. Towards usage control models: Beyond traditional access control [C] //Proc of the 7th ACM Symp on Access Control Models and Technologies. New York: ACM, 2002: 52-61

[3] Sahai A, Waters B. Fuzzy identity-based encryption [C] // Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 57-64

[4] Green M, Hohenberger S, Waters S. Outsourcing the decryption of ABE ciphertexts [C] //Proc of the 20th USENIX Conf on Security. Berkeley, CA: USENIX Association, 2011: 34-34

[5] Zhou Zhibin, Huang Dijiang. Efficient and secure data storage operations for mobile cloud computing [C] //Proc of the 8th Int Conf on Network and Service Management. New York: ACM, 2012: 37-45

[6] Li Jin, Huang Xinyi, Li Jingwei, et al. Securely outsourcing attribute-based encryption with checkability [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 8(25): 2201-2210

[7] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 28th IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Compter Society, 2007: 321-324

[9] Yu Shucheng, Wang Cong, Ren Kui, et al. Attribute based data sharing with attribute revocation [C] //Proc of the 5th ACM Symp on Information, Computer and Communications Security (ASIACCS'10). New York: ACM, 2010: 261-270

[10] Hohenberger S, Waters B. Online/offline attribute-based encryption [C] //Proc of PublicKey Cryptography (PKC 2014). Berlin:Springer, 2014: 293-310

[11] Wang Hao, He Debiao, Shen Jian, et al. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing [J]. Soft Computing, 2017, 21(24): 7325-7335

[12] Fan Kai, Wang Junxiong, Wang Xin, et al. A secure and verifiable outsourced access control scheme in fog-cloud computing [J]. Sensors, 2017, 17(7): 1695-1710

[13] Zhang Rui, Ma Hui, Lu Yao. Fine-grained access control system based on fully outsourced attribute-based encryption [J]. Journal of Systems and Software, 2017, 125(C): 344-353

[14] Li Jiguo, Sha Fengjie, Zhang Yichen, et al. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length [OL]. [2019-05-01]. http://www.en.cnki.com.cn/Article_en/CJFDTotal-HDZJ201603031.htm

[15] Zhao Zhiyuan, Wang Jianhua, Xu Kaiyong, et al. Fully outsourced attribute-based encryption with verifiability for cloud storage [J]. Journal of Computer Research and Development, 2019, 56(2): 442-452 (in Chinese)
(赵志远, 王建华, 徐开勇, 等. 面向云存储的支持完全外包属性基加密方案[J]. 计算机研究与发展, 2019, 56(2): 442-452)

[16] Chaum D, Pedersen T P. Wallet databases with observers [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 1995: 89-105

[17] Hohenberger S, Lysyanskaya A. How to securely outsource cryptographic computations [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2005: 264-282

[18] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Advances in Cryptology (CRYPTO 2010). Berlin: Springer, 2010: 465-482

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

[20] Dong Min, Ren Yanli, Zhang Xinpeng. Fully verifiable algorithm for secure outsourcing of bilinear pairing in cloud computing [J]. KSII Transactions on Internet & Information Systems, 2017, 11(7): 3648-3663

[21] Chen Xiaofeng, Susilo W, Li Jin, et al. Efficient algorithms for secure outsourcing of bilinear pairings [J]. Theoretical Computer Science, 2015, 562: 112-121

[22] Yu Yunpeng, Luo Yuchuan, Wang Dongsheng, et al. Efficient, secure and noniterative outsourcing of large-scale systems of linear equations [C] //Proc of 2016 IEEE Int Conf on Communications (ICC 2016). Piscataway, NJ: IEEE, 2016: 1-6

[23] Kumar M, Meena J, Tiwari S, et al. Privacy preserving, verifiable and efficient outsourcing algorithm for regression analysis to a malicious cloud [J]. Journal of Intelligent & Fuzzy Systems, 2017, 32(5):3413-3427

[24] Even S, Goldreich O, Micali S. On-line/off-line digital signatures [C] //Proc of Advances in Cryptology (CRYPTO'89). Piscataway, NJ: IEEE, 1989: 263-275

[25] Shamir A, Tauman Y. Improved online/offlfflffline signature schemes [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2001: 355-367

[26] Guo Fuchun, Mu Yi, Chen Zhide. Identity-based online/offline encryption [G] //Information Security and Privacy. Berlin: Springer, 2015

Gao Jiaxin, born in 1994. Master candidate. Her main research interests include cloud security and cryptography.

Sun Jiameng, born in 1990. PhD. His main research interests include cloud security and cryptography.

Qin Jing, born in 1960. Professor and PhD supervisor. Her main research interests include computational number theory, information security, design and analysis of security about cryptologic protocols.