

一种云存储下多授权访问控制及用户属性撤销方案

江泽涛^{1,2}, 王伟峰^{1,2}

(1 桂林电子科技大学 广西图像图形处理智能处理重点实验室, 广西 桂林 541004;

2 桂林电子科技大学 广西高校图像图形智能处理重点实验室, 广西 桂林 541004)

摘 要: 云存储下已有基于属性加密的访问控制研究多是基于单授权中心来实现, 该种方案在授权方不可信或遭受恶意攻击的情况下可能会造成密钥泄露。基于 CP-ABE 设计了一种多授权访问控制方案, 引用代理服务器 (Proxy Server, PS), 帮助用户承担大量解密操作; 对用户属性撤销问题采用高效安全的算法进行处理; 最后, 利用双线性判定 (Decision Bilinear Diffie-Hellman, DBDH) 假设理论证明是选择明文攻击安全的。

关键词: 云存储; 多授权中心; 访问控制; CP-ABE; 属性撤销

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2018)05-0055-06

A Scheme of Multi-authorization Access Control and User Attribute Revocation in Cloud Storage

JIANG Ze-tao^{1,2}, WANG Wei-feng^{1,2}

(1 The Key Laboratory of Image and Graphic Intelligent Processing of Guangxi, Guilin University of Electronic Technology, Guilin 541004, China; 2 The Key Laboratory of Image and Graphic Intelligent Processing of Higher Education in Guangxi, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: The research of access control based on attribute encryption has been implemented in cloud storage, which is mostly based on single authorization center, may result in the leakage of key. Proposing a CP-ABE design of a multi access control scheme based on reference proxy server (Proxy Server, PS), to help users to undertake a large number of decryption operation; Problems with high security attributes revocation algorithm for processing; Finally, using the bilinear decision (Decision Bilinear Diffie-Hellman, DBDH) proved to be the chosen plaintext attack security.

Key words: cloud storage; multi-authorization center; access control; CP-ABE; attribute revocation

1 引言

云存储是从云计算概念衍生和发展起来的新技术之一, 它通过网络将大量各种不同类型的存储设备集合在一起协同运作, 为用户提供在线数据存储服务^[1]. 在不可信云存储环境中, 用户将共享数据加密存储, 并通过对解密密钥的获取来实现密文访问控制. 基于属性加密 (ABE) 的方法被认为是解决云存储中数据安全和共享的有效加密机制^[2]. 在基于

CP-ABE 的云计算访问控制方案中, 用户撤销是一大难题. 洪澄等^[3]提出一种密文访问控制方法 HCRE, 其思想是设计一种基于秘密共享方案的算法, 将访问控制策略变更导致的重加密过程转移到云端执行, 只是系统属性撤销时需要同时更新系统的公开参数和用户私钥来完成即时性的权限撤销. 陈燕俐等^[4]提出的云计算访问控制方案中, 密文加密采用借助线性秘密共享矩阵的 CP-ABE 加密算法, 并将大部分密文重加密工作转移给云服务提供

收稿日期: 2017-07-22; **修回日期:** 2017-08-30

基金项目: 国家自然科学基金(61572147); 广西科技计划项目(AC16380108); 桂林电子科技大学图像图形智能处理重点实验室项目(GIIP201501); 广西可信软件重点实验室项目(kx201502); 研究生教育创新计划项目(YJCXS201536)

商执行,在用户属性撤销时,引入 SD 广播加密技术.但也造成数据属主的负担增加,密钥分发效率降低;关志涛等^[5]提出一种多授权中心访问控制模型 PRM-CSAC,设计了最小化属性分组算法,使用户访问文件时,能够按需分配密钥,但多访问树的设计无疑增加文件加密的复杂性和存储、传输的负担;周鹏旭等^[6]提出的方案 HE-MA-ACS 在层次化授权结构基础上,引入外包解密思想,将用户访问的大部分解密计算开销外包至云服务端.但在用户属性动态变化时,实现的是用户层面的撤销而不是属性层面的撤销.

本文针对现有多授权中心方案的不足,在文献^[7]基础上基于 CP-ABE 设计一种多授权中心访问控制方案,减少加解密计算量;对用户属性撤销问题借鉴文献^[8]的方法,实现高效的属性撤销.

2 系统模型框架和安全模型定义

2.1 系统模型和框架

本文系统包含 6 个实体:云服务提供商(Cloud Service Provider, CSP)、全局认证中心(Global Certificate Authority, GCA)、属性权威(Attribute Authorities, AAs)、数据拥有者(Data Owner, DO)、用户(User)和代理服务器(Proxy Server, PS). 系统模型如图 1 所示

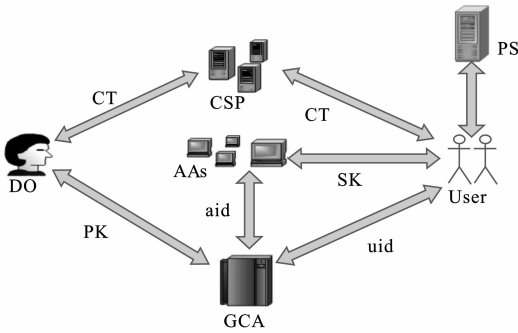


图 1 系统模型

GCA 为全局可信认证权威,为每个 AA 分配一个全局唯一身份标识,也为每一个合法用户分配一个全局唯一用户身份.

每个 AA 都是一个独立的属性权威,根据 User 的角色或身份负责用户属性的分发、撤销和更新任务. CSP 只存储 DO 加密的数据,并且提供 User 数据访问服务. DO 先采用对称加密机制对数据进行加密,再采用 CP-ABE 机制对对称密钥加密,得到密钥密文.然后,将两种密文一同上传并存储 CSP 中.

PS 管理大部分解密计算工作,其中我们认为 CSP 和 PS 之间没有直接联系. User 从 CSP 中下载密文,根据自身密钥在 PS 协助下解密得到需要访问的数据原文.

本系统主要包含如下算法:GCASetup1, AA-Setup, GCASetup2, Encrypt, KeyGen, Decrypt 和属性撤销算法:UKeyGen, SKUpdate, CTUpdate.

$GCASetup1(\lambda) = \{SP, MK, sk_{CA}, vk_{CA}, \{uid, uid.Cert, aid, aid.Cert\}\}$:

GCA 初始化算法 1 由 GCA 执行,输入安全参数 λ ,生成主密钥 MK,系统参数 SP,一对用来标识和认证 GCA 的全局公私钥 sk_{CA} 和 vk_{CA} 以及用户、属性权威 AA 的唯一标识和认证信息 $uid, uid.Cert, aid, aid.Cert$.

$AASetup(aid) = \{sk_{aid}, pk_{aid}, \{v_{x_{aid}}, pk_{x_{aid}}\}\}$: AA 初始化算法由每个 AA 单独运行,输入 AA 对应身份标识 aid ,生成一对属性权威的公私钥 sk_{aid} 和 pk_{aid} ,以及对于任意 $x \in AA_{aid}$ 的版本号和属性公钥 $\{v_{x_{aid}}, pk_{x_{aid}}\}$.

$GCASetup2(pk_{aid}) = \{PK\}$:当获得 pk_{aid} , GCA 运行此算法计算生成全局公钥 PK.

$Encrypt(m, SP, \phi, (M, \rho), \{PK_k\}_{k \in I_A}, \{PK_{x_k}\}_{x_k \in SA_k}) = \{CT\}$:加密算法由 DO 运行,对于明文信息 m ,先用对称密钥 ϕ 进行加密.输入系统参数 SP,属性权威公钥集 $\{PK_k\}_{k \in I_A}$,属性公钥集 $\{PK_{x_k}\}_{x_k \in SA_k}$ 和 (M, ρ) ,其中 M 为一个 $l \times n$ 的 LSSS 矩阵, ρ 是一个映射函数,将 M 的每一行映射为一个属性,最后生成密文 CT.

$KeyGen(SP, sk_{aid}, S_{uid, aid}, uid.Cert, \{PK_{x_{aid}}\}) = SK_{uid, aid}$:私钥生成算法由每个 AA 独立运行,输入系统参数 SP,一系列描述私钥的属性集 $S_{uid, aid}$,属性权威的私钥 sk_{aid} 和属性的公钥集 $\{PK_{x_{aid}}\}$,以及用户认证信息 $uid.Cert$,生成对应 uid 标识的用户私钥 $SK_{uid, aid}$.

$Decrypt(s, CT, SK_{uid, aid}) = \{\phi \text{ 或 } \perp\}$:解密算法由代理服务器 PS 和用户共同协作运行,输入隐藏的秘密参数 s ,密文 CT 和私钥 $SK_{uid, aid}$,计算得到对称密钥 ϕ .

$UKeyGen(SK_{aid}, \{u_j\}, \tilde{v}_{x_{aid}}) \rightarrow (KUK_{j, \tilde{x}_{aid}}, CUK_{\tilde{x}_{aid}})$:密钥生成算法由撤销属性 $\tilde{x}_{aid}$ 对应 AA 运行,输入私钥 SK_{aid} ,用户集 $\{u_j\}$ 和撤销属性之前版本号 $\tilde{v}_{x_{aid}}$,结果输出用户私钥更新密钥 $KUK_{j, \tilde{x}_{aid}}$ ($j \in S_U, j \neq \mu, \tilde{x}_{aid} \in S_{j, aid}$) 和密文更新密钥 $CUK_{\tilde{x}_{aid}}$.

$SK_{uid, aid} \leftarrow SK_{uid, aid} \cdot KUK_{uid, v_{x_{aid}}}$: 用户私钥更新算法由所有未撤销用户执行, 输入当前私钥 $SK_{uid, aid}$ 和更新钥匙 $KUK_{uid, v_{x_{aid}}}$, 输出一个新私钥 $SK_{uid, aid}$.

$CT_{update}(CT, CUK_{x_{aid}}) \rightarrow CT$: 密文更新算法由 CSP 运行, 输入当前密文 CT 和更新钥匙 $CUK_{x_{aid}}$, 输出一个新密文 CT .

2.2 安全模型定义

2.2.1 安全假设

本系统中, 安全假设为: CSP 是“honest but curious”的, 使用此模型将存在 CSP 和恶意用户共谋攻击的可能. GCA 假设是可信的, 但也可能对敌手 (例如 AAs) 妥协. 对于 DO 和 PS, 假设是完全可信的.

2.2.2 安全模型

假设存在一个敌手和一个挑战者, 挑战者提供基于访问策略的加密密文, 并向敌手隐藏具体信息. 过程描述如下:

(1) 初始化

挑战者在系统中运行系统初始化算法;

(2) 私钥查询阶段 1

敌手向挑战者提交属性集进行 S 私钥查询, 但是这些属性并不满足访问结构, 挑战者运行属性密钥生成算法, 生成对应属性私钥, 并交给敌手;

(3) 挑战

敌手提交两个等长明文 M_0, M_1 , 挑战者从敌手得到访问结构 $\dot{M}$, 在阶段 1 已知属性集 S 不满足 $\dot{M}$. 挑战者随机选取一个明文用 M_β 表示, 然后基于 $\dot{M}$ 加密并提交给敌手;

(4) 私钥查询阶段 2

敌手重复阶段 1, 只要属性集 S 不满足访问策略 $\dot{M}$, 可查询更多私钥信息;

(5) 猜测

敌手给出 β 的猜测结果 β' , 如果 $\beta' = \beta$, 则赢得游戏, 游戏中敌手称为选择明文攻击, 敌手优胜概率为 $\Pr[\beta' = \beta] - \frac{1}{2}$.

定义 1 本方案使用选择性明文安全假设, 即任意多项式时间内, 如果敌手在安全游戏中优势是可忽略的, 则方案是安全的.

3 具体方案

3.1 方案概括

考虑到冗杂的多个授权权威, 引用 Pedersen 等^[9]提出的 (t, n) 阈值秘密共享方法. AAs 首先向 CA 提出申请注册, 并帮助 CA 完成系统参数的生成过程. CA 对每个合法用户进行注册和颁发证书, DO 共享数据必须从 CA 中得到公钥, 然后基于预定义的访问策略对数据加密, 再将 CT 上传到 CSP. 只有用户属性集满足密文中隐藏的访问策略才能解密, 顺利得到数据明文.

3.2 方案详细描述

3.2.1 系统初始化

过程大致分为 3 个部分: GCASetup1, AASetup 和 GCASetup2.

(1) GCASetup1

由 GCA 运行, 选择两个一样素数阶 p 的多倍循环群 G 和 G_T , 定义一个双线性映射 $e: G \times G \rightarrow G_T$; 随机选择 $a \in Z_p$ 为主密钥, 计算相关部分公钥 g^a , 生成一对密钥 (sk_{CA}, vk_{CA}) 用于标识和认证, 为每个属性 $Att_i (i = 1, 2, \dots, U)$ 生成公钥: $h_1, h_2, \dots, h_U \in G$.

用户注册: 每个用户向 GCA 发送注册请求, GCA 验证用户信息通过, 分配用户唯一身份标识 $uid \in Z_p$ 和证书 $uid.Cert$.

AA 注册: 同样对于每个合法 AA, GCA 分配唯一身份标识 $aid \in Z_p$ 和证书 $aid.Cert$.

(2) AA Setup:

每个 $AA_i (i = 1, 2, \dots, n)$ 选择一个随机数 $\alpha_i \in Z_p$, 主密钥 α 表示为: $\alpha = \sum_{i=1}^n \alpha_i$. 随机生成一个 $t-1$ 阶的多项式 $f_i(x)$, 满足 $\alpha_i = f_i(0)$; AA_i 计算 $s_{ij} = f_i(aid_j)$, $(j = 1, 2, \dots, i-1, i+1, \dots, n)$, 并将结果安全发送给 AA_j , 同样 AA_i 计算 $s_{ii} = f_i(aid_i)$.

然后 AA_i 计算得到主密钥 $sk_i = \sum_{j=1}^n s_{ji}$ 和部分共享公钥: $pk_i = e(g, g)^{sk_i}$.

(3) GCASetup2

同样由 GCA 执行, 计算全局公钥:

$$\begin{aligned} e(g, g)^a &= e(g, g)^{\sum_{i=1}^t (sk_i \prod_{j=1, j \neq i}^{t-1} \frac{aid_j}{aid_j - aid_i})} \\ &= \prod_{i=1}^t e(g, g)^{sk_i \prod_{j=1, j \neq i}^{t-1} \frac{aid_j}{aid_j - aid_i}} \\ &= \prod_{i=1}^t pk_i \prod_{j=1, j \neq i}^{t-1} \frac{aid_j}{aid_j - aid_i} \end{aligned}$$

最后得到 $PK = (g, g^a, e(g, g)^a, n, t, h_1, h_2, \dots, h_U)$, 而 $MK = (a, \alpha)$ 隐藏在系统中.

3.2.2 加密

由 DO 执行, 先随机选择 $\phi \in Z_p$ 作为对称密钥, 对称加密算法例如 (AES) 对明文 m 使用 ϕ 加密, 表示为 $E_\phi(M)$; 然后基于 CP-ABE 算法对对称密钥 ϕ 加密, 用到 LSSS 访问结构 (M, ρ) , M 是一个 $l \times n$ 的矩阵, 函数 ρ 将 M 每一行映射为一个对应属性. 随机选择 $r_1, r_2, \dots, r_l \in Z_p$, 计算密文 CT:

$$\begin{aligned} CT &= (C = \phi e(g, g)^\alpha, \hat{C} = g^s), \\ \forall i &= 1 \rightarrow l, C_i = (g^a)^{\lambda_i} \cdot h_{\rho(i)}^{-r_i}, D_i = g^{r_i}. \end{aligned}$$

接着 DO 将 $E_\phi(M)$ 和 CT 一起发送给 CSP.

3.2.3 私钥生成

选择一个随机数 $b_i \in Z_p$, 表示:

$$K_i = g_i^{\text{sk}} \cdot g^{b_i}, L_i = g^{b_i}, \forall \text{Att}_i \in S: K_{\text{Att}_i} = h_{i, \text{Att}_i}^{b_i}.$$

私钥生成过程:

$$\begin{aligned} K &= \prod_{i=1}^t (g_i^{\text{sk}} \cdot g^{b_i}) \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i} \\ &= \prod_{i=1}^t ((g_i^{\text{sk}}) \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i} \cdot (g^{b_i}) \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i}) \\ &= g^a \cdot g^{\sum_{i=1}^t (b_i \cdot \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i})}, \\ L &= g^{\sum_{i=1}^t (b_i \cdot \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i})}, \\ \forall \text{Att} \in S: K_{\text{Att}} &= h_{\text{Att}}^{\sum_{i=1}^t (b_i \cdot \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i})}. \end{aligned}$$

$$\text{引用参数 } d = \sum_{i=1}^t (b_i \cdot \prod_{j=1, j \neq i}^t \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i}),$$

最后得到简化公式:

$$K = g^a \cdot g^{a \cdot d}, L = g^d, \forall \text{Att} \in S: K_{\text{Att}} = h_{\text{Att}}^d.$$

3.2.4 解密

由用户和代理服务器 PS 一起完成, 存在一个适当参数 $\{\omega \in Z_p\}_{i \in I}$ 满足 $\vec{e} = (\omega_1, \omega_2, \dots, \omega_{|I|}) M_U$, 用户计算隐藏秘密参数 s :

$$\begin{aligned} s &= (1, 0, \dots, 0) \cdot (s, y_2, \dots, y_n)^T \\ &= \vec{e} \vec{v}^T = (\omega_1, \omega_2, \dots, \omega_{|I|}) M_U \cdot \vec{v}^T \\ &= (\omega_1, \omega_2, \dots, \omega_{|I|}) \vec{\lambda}_I^T = \sum_{i \in I} \omega_i \cdot \lambda_i. \end{aligned}$$

这里 $\vec{\lambda}_I^T$ 表示 $(\lambda_1, \lambda_2, \dots, \lambda_l)$ 的子向量, 由 PS 执行, 计算:

$$\begin{aligned} C_U &= \frac{e(\hat{C}, K)}{\prod_{i \in I} (e(C_i, L) \cdot e(D_i, K_{\rho(i)}))^{\omega_i}} \\ &= \frac{e(g^s, g^a \cdot g^{a \cdot d})}{\prod_{i \in I} (e((g^a)^{\lambda_i} \cdot h_{\rho(i)}^{-r_i}, g^d) \cdot e(g^{r_i}, h_{\rho(i)}^d))^{\omega_i}} \\ &= \frac{e(g, g)^{a \cdot s} \cdot e(g, g)^{a \cdot s \cdot d}}{\prod_{i \in I} e(g, g)^{d \cdot a \cdot \lambda_i \cdot \omega_i}} = e(g, g)^{as} \end{aligned}$$

PS 将结果再返还给用户, 得到对称密钥: $\phi = \frac{C}{C_U}$

$$= \frac{C}{e(g, g)^{as}}, \text{最后用户通过解密对称密钥得到明文 } M.$$

3.2.5 属性撤销和更新

假设用户 U_μ 的一个属性 $\tilde{x}_k$ 从 AA_k 中被撤销, 大概分为三个阶段:

阶段 1: 密钥生成更新

对应的授权权威 AA_k 运行 UKeyGen 算法, 生成一个新的属性版本号 $\dot{VK}_{\tilde{x}_k} = \dot{v}_{\tilde{x}_k}$, 计算属性更新密钥为 $AUK_{\tilde{x}_k} = \gamma_k (\dot{v}_{\tilde{x}_k} - v_{\tilde{x}_k})$, 得到用户私钥更新密钥 $KUK_{j, \tilde{x}_k} = g^{u_j \beta_k \cdot AUK_{\tilde{x}_k}}$ 和密文更新密钥 $CUK_{\tilde{x}_k} = \frac{\beta_k}{\gamma_k} \cdot AUK_{\tilde{x}_k}$; 并更新撤销属性的公钥为 $PK_{\tilde{x}_k} = PK_{\tilde{x}_k} \cdot g_{x_k}^{AUK}$, 将公钥已更新的信息传播给所有 DO.

阶段 2: 私钥更新

对于未撤销用户 $U_j (j \in S_U, j \neq \mu)$, 有属性 $\tilde{x}_k$, 接受 AA_k 发送的 $KUK_{j, \tilde{x}_k}$, 计算 SKUpdate:

$$\begin{aligned} SK_{j, k} &= (\dot{K}_{j, k} = K_{j, k}, \dot{L}_{j, k} = L_{j, k}, \dot{K}_{j, \tilde{x}_k} = K_{j, \tilde{x}_k} \\ &\cdot KUK_{j, \tilde{x}_k}, \end{aligned}$$

$$\forall x \in S_U, x \neq \tilde{x}_k: \dot{K}_{j, k} = K_{j, k}).$$

阶段 3: 密文更新

同样 CSP 接受 AA_k 发送的 CTUpdate, 运行 CTUpdate 算法输出新密文 CT' :

$$\begin{aligned} CT &= (C = \phi e(g, g)^\alpha, \hat{C} = g^s, \forall i = 1 \rightarrow l: \\ \text{若 } \rho(i) &\neq \tilde{x}_k: C_i = g^{a \lambda_i} \cdot h_{\rho(i)}^{-r_i}, D_i = g^{r_i}, \\ \text{若 } \rho(i) &= \tilde{x}_k: \dot{C}_i = C_i \cdot D_i^{CUK_{\tilde{x}_k}}, D_i = g^{r_i}). \end{aligned}$$

4 安全和技术性能分析

4.1 访问策略安全分析

为证明方案中访问策略的安全性, 使用定理:

定理 1 决定性 q-BDHE 假设成立时, 不会存在敌手用带有大小为 $\dot{l} \times \dot{n}$ 的挑战矩阵运行多项式时间算法选择攻击方案成功的, 其中 $\dot{l} \times \dot{n} \leq q$.

证明: 假设敌手 ψ 在安全游戏中具有不可忽视

的优势 $\epsilon = Adv_\psi$, 随机选择矩阵 $\dot{M}$ 进行挑战. 敌手 ψ 能查询任何不能直接用于解密密文的私钥, 挑战者将 AAs 生成的共享私钥和为敌手生成的私钥隐藏. 此安全游戏可被当做单个授权权威一样对待, 所以我们也建立一个模拟器 Γ 用于处理决定性 q-BDHE 问题, 由于本文方案的访问策略与 TMACS^[7] 整体上相近, 所以详细证明过程见文献[7].

4.2 抗共谋攻击安全

定理 2 本方案在抗共谋攻击上是安全的.

证明:每个用户在系统中都被赋予一个全局唯一身份 uid,对于同一用户被不同 AAs 分配的私钥都和 uid 相关;并且由于每个 AA 唯一身份 aid 的存在,因此所有属性是可分辨的.解密操作是用户和代理服务器共同完成,而代理服务器假设是可信的,进一步阻碍合谋解密;而本文在私钥中使用随机元素 $d = \sum_{i=1}^t (b_i \cdot \prod_{j=1, j \neq i}^t \frac{aid_j}{aid_j - aid_i})$,使不同用户的同一属性对应私钥是可分辨的,因此他们不会结合彼此私钥获得更多隐私信息.

4.3 性能分析

本文从用户的角度,将所提方案同 MA-ABE^[10]和 TMACS^[7]作对比,得出结果如表 1、表 2 所示.

表 1 存储开销

实体	CA	AA	Owner	User
本方案	$[2(U+N_U)+n+10] p $	$(2U+6) p $ (每个 AA)	$(2U+4) p $	$5 p $
MA-ABE	$[3(U+N_U)+n+4] p $	$2(U+N_U) p $	$(2U+4) p $	$(2N_{uid}+10) p $
TMACS	$[2(U+N_U)+n+10] p $	$(2U+6) p $ (每个 AA)	$(2U+4) p $	$(5+2N_{uid}) p $

表 2 计算开销

方案	授权中心	加密时间	解密时间	属性撤销控制者	解密控制者
本方案	多授权	$(2S+4)E$	$ I P+ I E$	AA	PS+User
MA-ABE	多授权	$(2S+1)E$	$2 I P+E$	Owner	User
TMACS	多授权	$(2S+4)E$	$2 I P+ I E$	—	User

5 结束语

本文提出一种多授权中心访问控制方案,大幅度减少用户解密计算负担,有效抵抗了共谋攻击;同时实现高效安全的属性撤销,在以后的工作中,会对本方案继续改进完善,使访问结构更加精简.

参考文献:

[1] 洪澄,张敏,冯登国. AB-ACCS:一种云存储密文访问控制方法[J]. 计算机研究与发展, 2010, 47 (sup1): 259-265.

[2] XIA Zhihua, ZHANG Liangao, LIU Dandan. Attribute-based access control scheme with efficient revocation in cloud computing[J]. 中国通信(英文版), 2016, 13(7):92-99.

[3] 洪澄,张敏,冯登国,等. 面向云存储的高效动态密文

令 $|p|$ 表示素数阶为 p 的群组元素大小, n 为 AAs 的数量, t 为阈值.假设 U 是属性总数量,则系统用户数量表示为 N_U , N_{uid} 表示身份为 uid 的用户所拥有属性的平均数量.另外 S 表示与密文相关的属性集, E 表示一次指数操作, I 表示用户属性集, P 表示一次配对操作.从表 1 得知,本方案和 TMACS 在存储开销方面普遍比 MA-ABE 较低,是因为访问策略采用的 LSSS 线性矩阵比 MA-ABE 采用的访问结构树更有优势,所占存储空间更小,而本方案解密大部分工作转移给 PS,减轻了用户的存储负担;表 2 体现了在解密计算开销上,本方案略占优势,并且由于属性撤销控制者是 AA,解密控制者是 PS 和 User,在一定程度上减少了 DO 和用户的计算负担,有助于抵抗共谋攻击.

访问控制方法[J]. 通信学报, 2011, 32(7):125-132.

[4] 陈燕俐,宋玲玲,杨庚. 基于 CP-ABE 和 SD 的高效云计算访问控制方案[J]. 计算机科学, 2014, 41(9): 152-157.

[5] 关志涛,杨亭亭,徐茹枝,等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6):116-126.

[6] 周鹏旭,李成海. 一种高效多授权中心云访问控制方案[J]. 计算机科学, 2016, 43(9):180-183.

[7] Li W, Xue K, Xue Y, et al. TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27 (5): 1484-1496.

[8] Yang K, Jia X, Ren K, et al. DAC-MACS: Effective data access control for multi-authority cloud storage systems[C]// INFOCOM, 2013 Proceedings IEEE. IEEE, 2014:2895-2903.

[9] Pedersen T P. A threshold cryptosystem without a trusted party[M]// Advances in Cryptology - EURO-CRYPT '91. Springer Berlin Heidelberg, 1994: 522-526.

[10] 李谢华,张蒙蒙,刘鸿,等. 基于 MA-ABE 的云存储访问控制方法 [J]. 湖南大学学报(自然科学版),

2015,29(10):133-140.

作者简介:

江泽涛 男,(1961-),教授,博士生导师.研究方向为访问控

制与信息安全及计算机视觉.

E-mail: 1459586819@qq. com.

王伟峰 男,(1992-),硕士研究生.研究方向为访问控制与信息安全.

(上接第 54 页)

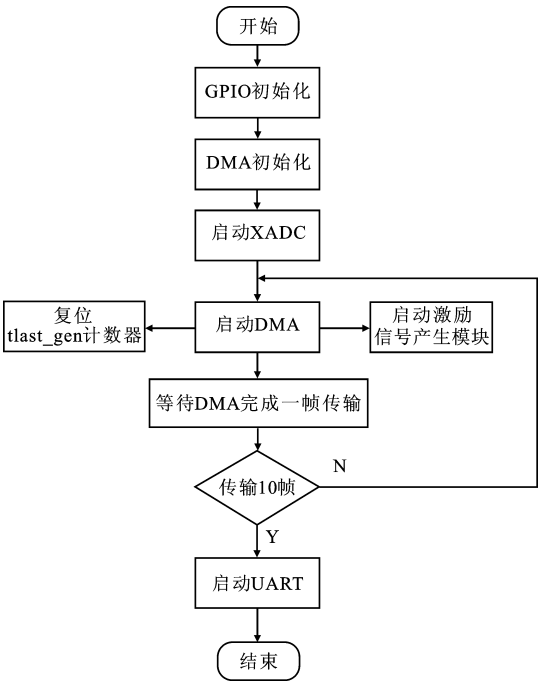


图 9 SOPC 软件工作流程图

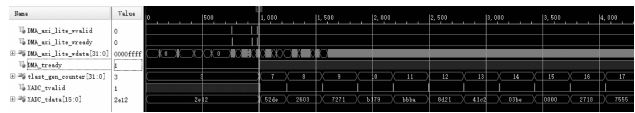


图 10 ILA 核抓取的硬件电路信号图

7 结束语

本文设计了一个用于手势识别的超声波收发器嵌入式系统,根据应用需要,设计了信号发射功率和采集端电压增益的调节机制、发射器的激励信号波形和驱动机制、发射信号和采集端采样 ADC 之间的同步触发机制以及回波数据的传输机制等.采用 SOPC 平台作为发射信号源和接收端控制器,利用

SOPC 的可编程性特点,可以根据不同的应用要求灵活定制发射信号的体制以及系统参数,实现不同的软硬件协同设计方案.通过实际的实验测试,验证了该系统的可行性和实用性,适合对超声波手势识别技术的开发.

参考文献:

[1] Skolnik M I. Introduction to radar systems[M]. New York City :Tata McGraw-Hill Education, 1980.

[2] Richards M A. Fundamentals of radar signal processing[M]. New York City :Tata McGraw-Hill Education, 2005.

[3] Alabaster C. Pulse doppler radar[J]. IEEE Aerospace & Electronic Systems Magazine , 2013, 28 (11) : 40-42.

[4] Murata Manufacturing Co. MA40S4S [EB/OL]. (2015-04-30). [2017-07-10]. <http://www.murata.com/zh-cn/products/productdata/8797589340190/MASPOPSE.pdf>.

[5] Murata Manufacturing Co. MA40S4R [EB/OL]. (2015-04-30). [2017-07-10]. <http://www.murata.com/zh-cn/products/productdata/8797589274654/MASPOPSE.pdf>.

作者简介:

杨建涛 男,(1990-),硕士研究生.研究方向为超声波手势识别系统设计. E-mail: yangjiantao5261@126. com.

李翔宇 男,(1977-),博士,副研究员.研究方向为高效 SOC 系统设计、传感器节点处理器、信息安全芯片.

王 硕 男,(1992-),硕士研究生.研究方向为雷达基带电路设计.

殷树娟 女,(1981-),博士,副教授.研究方向为混合信号电路设计.