

一种高效多授权中心云访问控制方案

周鹏旭 李成海

(空军工程大学防空反导学院 西安 710051)

摘要 针对已有云计算多授权访问控制方案中用户端负担过重的问题,提出一种基于属性加密的多授权中心访问控制方案 HE-MA-ACS。在层次化授权结构的基础上,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,实现细粒度的属性撤销,并且用户端不需要参与属性的撤销操作。对方案的正确性、安全性、计算和存储性能进行了分析,证明了该方案在用户端存储开销、访问通信开销、解密时间及属性撤销时计算开销上的优越性。该方案有效地降低了用户端的负担,提高了解密效率。

关键词 多授权中心,属性基加密,云计算,访问控制,外包解密

中图分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.9.035

High Efficiency Multi-authority Cloud Access Control Scheme

ZHOU Peng-xu LI Cheng-hai

(School of Air and Missile Defense, Air Force Engineering University, Xi'an 710051, China)

Abstract For solving the overhead problems of users in the multi-authority access control schemes, a HE-MA-ACS scheme was proposed. Outsourced decryption is introduced based on the hierarchical authorization structure, so large part of the decryption overhead is moved to the CSP. Furthermore, fine-grained attribute revocation is achieved and the users can not participate in the operation when their attributes are revoked. The correctness, security, calculated and storage performance were analyzed. Experimental results demonstrate the superiority of overhead in user storage, access communication, decryption and the computation costs when attribute is revoked as well. The scheme effectively reduces the burden on the user side and improves the efficiency of decryption.

Keywords Multi-authority, ABE, Cloud computing, Access control, Outsourced decryption

云计算(Cloud Computing)自面世以来便获得了工业界、学术界和政府等各界的广泛关注^[1],可以为用户提供高可扩展性、动态的、高效的、高性价比的服务^[2]。但是,新的安全问题也随这一模式而出现,用户数据存储在“honest but curious”^[3]的CSP(Cloud Service Provider)端,CSP可能由于商业目的将用户的数据提供给未授权的第三方,或者自己窃取或修改用户数据,对用户隐私构成极大威胁,这也是目前云计算要获得广泛应用所面临的重要问题,即如何保证用户数据在服务端的机密性、完整性和可用性。

为了解决云计算所面临的安全问题,相关人员进行了深入研究,并且取得了一定成果。Sahai A等^[4]于2005年首次提出了FIBE(Fuzzy Identity-Based Encryption)方案,首次将生物学特征直接作为身份信息用于加密操作中。2006年,Goyal V等^[5]在此基础上提出了KP-ABE(Key-Policy Attribute-Based Encryption)方案,用以实现用户对加密数据的细粒度访问。2007年,Bethencourt J等^[6]在文献[4]的基础上又提出了CP-ABE(Ciphertext-Policy Attribute-Based Encryption)方案,该方案的访问策略由数据发送方决定,适合于云计算环境中的应用。温昱晖等^[7]针对传统的CP-ABE机制中

用户访问数据的权限无法有效撤销的问题,提出了基于CP-ABE-R的数据访问控制云安全方案,其为每个用户分配一个唯一标识符,并按照给定的时戳发布吊销信息,有效地解决了用户吊销机制问题。

上述各种方案都是基于单授权中心实现的。在单授权中心方案中,系统中的每个用户都需要在一个可信的授权中心处注册并获取私钥;在大规模云服务应用中,单授权中心需要管理大量的用户属性,容易造成系统瓶颈,这样就需要多授权中心来对用户的属性进行分块管理。Chase^[8]最早提出多授权中心的概念,在此概念的基础之上给出基于属性的加密方案,用户的不同属性由多个授权中心分别进行管理,并生成对应属性的加密私钥。在Sushmita等^[9]提出的方案中,作者不采用一个可信的CA来对系统进行构建,数据拥有者和用户的属性授予及私钥的生成与分发由KDCs(Key Distribution Centers)来实现,该方案的缺点是用户需要承担大量的解密开销。Liu等^[10]提出一种层次化的属性基访问控制方案,该方案将CP-ABE算法与ABS(Attribute-based Signature)机制相结合,实现权限管理和对资源进行访问控制的功能,但是同样要求用户端对密文进行解密,加重了用户的计算负担。

到稿日期:2016-01-05 返修日期:2016-04-04

周鹏旭(1991—),男,硕士生,主要研究方向为网络与信息安全,E-mail:zhoupengxu2015@sina.com;李成海(1966—),男,硕士,教授,主要研究方向为网络与信息安全。

本文针对已有多授权中心方案的不足,借鉴李勇等^[16]提出的方法,对 Yang 等^[17]提出的方案进行改进,提出 HE-MA-ACS 方案,即实现将解密密钥的一部分存放在 CSP 端,另一部分存放在用户端,当用户访问数据时,由 CSP 首先对密文进行部分解密,使得用户端的解密计算量降低,同时用户端对密钥的存储开销及用户访问数据时的数据通信量都得到降低。当有属性进行撤销时,私钥和密文的升级操作发生在 CSP 端,对用户来说是透明的。

的行构成的子集,同时要求由 VUV_{aid} 构成的子空间不能包含 $(1,0,\dots,0)$ 。挑战者随机掷币 $b \in \{0,1\}$,然后利用 (M^*, ρ^*) 对 M_b 进行加密,并将所得密文 CT^* 发送给敌手。

阶段2 敌手可以重复阶段1的工作,在如下限制条件下查询更多的私钥和更新密钥。

敌手不能直接查询 CT^* 的解密密钥或通过将来自 S_A 的任何密钥进行组合来解密 CT^* ;同时不能通过查询私钥更新密钥来获得 CT^* 的解密密钥。即敌手不能通过查询的方式直接或间接地对 CT^* 进行解密。

猜测阶段:敌手输出对 b 的猜测 b' 。

敌手在上述游戏中的优势定义为 $\Pr[b=b'] - \frac{1}{2}$ 。

定义2(安全性定义) HE-MA-ACS 方案是安全的,当且仅当在上述攻击游戏中,任何多项式时间的敌手的攻击优势是可以忽略的。

2 具体方案

2.1 具体实现

设 q 是一个大素数, G_1 是阶为 q 的循环群, g 是 G_1 的生成元, $e: G_1 \times G_1 \rightarrow G_2$ 为一个双线性映射, $H: \{0,1\}^* \rightarrow G_1$ 为一个哈希函数。

CASetup(a): CA 随机选取 $a \in Z_q$ 作为系统主密钥 MSK,计算 $SP = g^a$;然后受理 AA 和用户的注册申请。

AA 注册申请:

每个 AA 在系统初始化时在 CA 处注册,CA 分配给 AA 一个权威身份标识 aid 。

AASetup(aid): 每个 $AA_k (k \in S_A)$ 独立运行初始化算法;随机选取 $\alpha_k, \beta_k, \gamma_k \in Z_q$ 生成其私钥 $SK_k = (\alpha_k, \beta_k, \gamma_k)$ 和公钥 $PK_k = (e(g, g)^{\alpha_k}, g^{\frac{1}{\beta_k}}, g^{\frac{1}{\gamma_k}})$ 。其所管理的所有属性组成集合 S_{A_k} ,对每个 $x_k \in S_{A_k}$,生成它的属性公钥 $PK_{x_k} = (g^{v_{x_k}} H(x_k))^{\gamma_k}$ 。

用户注册申请:

每个用户在系统初始化时在 CA 处注册,CA 分配给用户一个全局唯一身份标识 uid ;随机选取 $u_{uid}, z_{uid} \in Z_q$,计算生成并传递给用户全局公钥 $GPK_{uid} = g^{uid}$ 和全局私钥 $GSK_{uid} = z_{uid}$,将 $\{uid, SP, g^{\frac{1}{z_{uid}}}\}$ 传递给 AAs。

Encrypt($SP, \{PK_k\}_{k \in I_A}, \{PK_{x_k}\}_{x_k \in S_{A_k}}, \psi, (M, \rho)$): 令 M 为一个 $l \times n$ 矩阵,其中 l 表示系统中所有属性的总数。函数 ρ 将 M 中的每行映射为一个属性。 I_A 表示与访问结构相关的属性权威集合。该算法首先产生一个随机矢量 $\vec{v} = (s, y_2, \dots, y_n) \in Z_q^n$,对 $i=1, \dots, l$,计算 $\lambda_i = \vec{v} \cdot M_i$,其中 M_i 是 M 中的第 i 行参数,然后随机选取 $r_1, r_2, \dots, r_l \in Z_q$,对信息 ψ 进行如下加密:

$$CT = \{C = \psi \cdot (\prod_{k \in I_A} e(g, g)^{\alpha_k})^s, C' = g^s, C'' = g^{\frac{s}{\beta_k}}, \forall i = 1 \text{ to } l; C_i = g^{\alpha_i} \cdot ((g^{v_{\rho(i)}} H(\rho(i)))^{\gamma_k})^{-r_i}, D_{1,i} = g^{\frac{r_i}{\beta_k}}, D_{2,i} = g^{-\frac{\gamma_k}{\beta_k} r_i}, \rho(i) \in S_{A_k}\}$$

KeyGen($SP, SK_{aid}, S_{aid}, aid, \{PK_{x_{aid}}\}$): $AA_k (k \in S_A)$ 根据用户 $U_j (j \in S_U)$ 在其管理域内的角色或身份为用户分配一个属性集 $S_{j,k}$;然后运行算法,生成用户的转换密钥:

$$TK_{j,k} = \{K_{j,k} = g^{\frac{\alpha_k}{z_j}} \cdot g^{a_{u_j}} \cdot g^{\frac{a_{t_{j,k}}}{\beta_k}}, L_{j,k} = g^{\frac{\beta_k}{z_j} t_{j,k}}, R_{j,k} = g^{a_{j,k}}, \forall x_k \in S_{j,k}: K_{j,x_k} = g^{\frac{\gamma_k}{z_j} t_{j,k}} \cdot (g^{v_{x_k}} \cdot H(x_k))^{\gamma_k (\beta_k u_j + \gamma_k^2)}\}$$

Transform($TK_{aid,aid}, CT$): 当 $TK_{aid,aid}$ 所对应的属性集不满足 CT 的访问策略时,输出 $\perp$,否则选择 $\{w_i \in Z_q\}_{i \in I}$ 对 s 进行重构,即 $s = \sum_{i \in I} w_i \lambda_i$;然后对密文进行转化:

$$\prod_{k \in I_A} \frac{e(C', K_{j,k}) \cdot e(R_{j,k}, C'')^{-1}}{(e(C_i, GPK_{U_j}) \cdot e(D_{1,i}, K_{j,\rho(i)}) \cdot e(D_{2,i}, L_{j,k} PK_{\rho(i)}))^{w_i N_A}} = \prod_{k \in I_A} e(g, g)^{\frac{\alpha_k}{z_j} s}$$

其中, $N_A = |I_A|$ 表示与密文相关的 AA_k 的总数, $I_A = \{i: \rho(i) \in S_{A_k}\}$,然后,将得到的 $CT^\wedge = \{C, \prod_{k \in I_A} e(g, g)^{\frac{\alpha_k}{z_j} s}\}$ 发送给用户。

Decrypt($CT^\wedge, GSK_{uid}$): 用户 U_j 利用自己的全局私钥 GSK_{uid} 对 $CT^\wedge$ 进行解密操作:

$$\psi = \frac{C}{(\prod_{k \in I_A} e(g, g)^{\frac{\alpha_k}{z_j} s})}$$

获得对称加密密钥。

2.2 属性撤销

AA_k 若想撤销用户 u_μ 的属性 x_k ,其版本号为 v_{x_k} ,为其随机选取并公布一个新版本号 v'_{x_k} 。计算生成未撤销该属性的用户的升级密钥 $UUK_{j,x_k} = g^{(u_j \beta_k + \gamma_k)(v'_{x_k} - v_{x_k})} (u_j \in S_U, j \neq \mu)$, S_U 表示系统中用户的集合。为访问控制策略中仍具有属性 x_k 的密文生成升级密钥 $CUK_{x_k} = \beta_k (v'_{x_k} - v_{x_k})$, AA_k 将 UUK_{j,x_k} 和 CUK_{x_k} 一并发送给 CSP,为仍具有属性 x_k 的用户更新转换密钥,并对相关密文进行升级。具体实现如下:

$$TK_{j,k}^* = \{K_{j,k}^* = g^{\frac{\alpha_k}{z_j}} \cdot g^{a_{u_j}} \cdot g^{\frac{a_{t_{j,k}}}{\beta_k}}, L_{j,k}^* = g^{\frac{\beta_k}{z_j} t_{j,k}}, R_{j,k}^* = g^{a_{j,k}}, \{K_{j,x_k}^* = g^{\frac{\gamma_k}{z_j} t_{j,k}} \cdot (g^{v_{x_k}} \cdot H(x_k))^{\gamma_k (\beta_k u_j + \gamma_k^2)}\} \forall x \in S_U, x \neq x_k, K_{j,x_k}^* = K_{j,x_k} \cdot UUK_{j,x_k}\}$$

$$CT^* = \{C^* = \psi \cdot (\prod_{k \in I_A} e(g, g)^{\alpha_k})^s, C'^* = g^s, C''^* = g^{\frac{s}{\beta_k}}, \{C_i^* = g^{\alpha_i} \cdot ((g^{v_{\rho(i)}} H(\rho(i)))^{\gamma_k})^{-r_i} \forall i = 1 \text{ to } l; \text{ if } \rho(i) \neq x_k, \text{ otherwise: } C_i^* = C_i \cdot g^{-\gamma_k r_i (v'_{x_k} - v_{x_k})}, D_{1,i}^* = g^{\frac{r_i}{\beta_k}}, D_{2,i}^* = g^{-\frac{\gamma_k}{\beta_k} r_i}, \rho(i) \in S_{A_k}\}\}$$

3 系统分析

3.1 正确性分析

方案中只有合法的用户才能最终获得对称解密密钥,进而获得数据明文:

$$\prod_{k \in I_A} \frac{e(C', K_{j,k}) \cdot e(R_{j,k}, C'')^{-1}}{(e(C_i, GPK_{U_j}) \cdot e(D_{1,i}, K_{j,\rho(i)}) \cdot e(D_{2,i}, L_{j,k} PK_{\rho(i)}))^{w_i N_A}} = \prod_{k \in I_A} e(g^s, g^{\frac{\alpha_k}{z_j}} \cdot g^{a_{u_j}} \cdot g^{\frac{a_{t_{j,k}}}{\beta_k}}) e(g^{a_{j,k}}, g^{\frac{1}{\beta_k}})^{-1} = \prod_{k \in I_A} e(g, g)^{s a_{u_j}} e(g, g)^{\frac{s a_k}{z_j}} = e(g, g)^{N_A s a_{u_j}} \cdot \prod_{k \in I_A} e(g, g)^{\frac{s a_k}{z_j}}$$

对于 $\{\rho(i)\}_{i \in I} \in S_k$, 计算

$$\begin{aligned} & \prod_{k \in I_A} \prod_{i \in I_{A_k}} (e(C_i, GPK_{U_j}) \cdot e(D_{1,i}, K_{j, \rho(i)}) \cdot e(D_{2,i}, L_{j,k} \\ & \quad PK_{\rho(i)}))^{w_i N_A} \\ &= \prod_{k \in I_A} \prod_{i \in I_{A_k}} (e(g^{a_i} \cdot ((g^{v_{\rho(i)}} H(\rho(i)))^{\gamma_k})^{-r_i}, g^{u_j}) \cdot \\ & \quad e(g^{\frac{r_i}{\beta_k}}, g^{\frac{\beta_k \gamma_k}{z_j}})^{z_j} \cdot (g^{v_{x_k}} \cdot H(\rho(i)))^{(\gamma_k \beta_k u_j + \gamma_k^2)}) \cdot \\ & \quad e(g^{\frac{-\gamma_k}{\beta_k}}, g^{\frac{\beta_k}{z_j}})^{z_j} (g^{v_{x_k}} H(\rho(i)))^{\gamma_k})^{w_i N_A} \\ &= \prod_{k \in I_A} \prod_{i \in I_{A_k}} (e(g, g)^{a_i u_j})^{w_i N_A} \\ &= e(g, g)^{N_A u_j \sum_{i \in I} w_i \lambda_i} \\ &= e(g, g)^{N_A u_j s} \end{aligned}$$

从而

$$\begin{aligned} & \prod_{k \in I_A} \frac{e(C', K_{j,k}) \cdot e(R_{j,k}, C')^{-1}}{\prod_{i \in I_{A_k}} (e(C_i, GPK_{U_j}) \cdot e(D_{1,i}, K_{j, \rho(i)}) \cdot e(D_{2,i}, L_{j,k} PK_{\rho(i)}))^{w_i N_A}} \\ &= \prod_{k \in I_A} e(g, g)^{\frac{a_{k,s}}{z_j}} \\ \text{进而, } \phi &= \frac{C}{(\prod_{k \in I_A} e(g, g)^{\frac{a_{k,s}}{z_j}})^{z_j}} = \frac{\psi \cdot (\prod_{k \in I_A} e(g, g)^{a_k})^s}{(\prod_{k \in I_A} e(g, g)^{\frac{a_{k,s}}{z_j}})^{z_j}}. \end{aligned}$$

3.2 安全性分析

HE-MA-ACS 方案是对文献[17]进行的改进, 安全威胁来自于用户解密密钥的分配, 本方案将原方案中存储于用户端的解密密钥的一部分转移至服务端保存并进行更新操作,

使服务端具备了随时可以部分解密密文和对用户转换密钥进行更新的能力。系统中数据明文的获得依赖于用户的全局私钥, 所以服务端随时解密密文的能力不会破坏系统的安全性; 当用户 u_μ 的属性 x_k 发生撤销时, 由于用户的升级密钥 $UUK_{j, x_k} = g^{(u_j \beta_k + \gamma_k) \gamma_k (v'_{x_k} - v_{x_k})}$ ($u_j \in S_U, j \neq \mu$), 其中 γ_k 通过 AA_k 的私钥来获取, CSP 无权限, 因此防止了用户通过与 CSP 的合谋来为自己的转换密钥升级, 即保证了本方案的安全性。同时解密密文时需要用户的全局私钥 GSK_{uid} , 所以不同的用户不可能通过合谋来获得他们各自无权限的数据明文。 AA_k 虽然为用户分发属性版本集并生成转换密钥, 但不同的 AA_k 之间因不具备用户 u_j 的全局私钥而无法通过合谋来获取与 u_j 相关的未授权明文信息。

3.3 性能分析

云计算作为一种服务模式, 用户在对服务安全性提出要求的同时, 对服务的性能也有较高的要求。本文从用户的角度, 将所提方案同 DAC-MACS 方案^[17]和 MMACS 方案^[18]作对比, 对存储开销、传输过程中的通信开销、解密时间以及属性撤销时用户的计算开销进行分析, 结果如表 1 所列。

令 $|q|$ 表示群 G_1, G_2 和 Z_q 中元素的长度, $n_{a,k,uid}$ 表示属性权威 AA_k 分配给 uid 的属性数, $|PA|$ 表示用户分配给用户属性数, 加密所涉及的属性数为 l , T_p 表示一次双线性对计算所用的时间, T_m 表示一次求幂运算所用的时间 (本文解密时间不包括对称解密时间)。

表 1 3 种方案的综合比较

方案	存储开销	访问通信开销	解密时间	解密承担者	属性撤销时计算开销
文献[17]方案	$(N_A + 1 + \sum_{k=1}^{N_A} n_{a,k,uid} + 2 PA) q $	$l q $	$(3l+3)T_p + lT_m$	Users	T_m
文献[18]方案	$(3N_A + 1 + \sum_{k=1}^{N_A} n_{a,k,uid}) q $	$(3N_A + D) q $	T_m	大部分外包至 CSP	T_m
本方案	$(1 + \sum_{k=1}^{N_A} n_{a,k,uid}) q $	$l q $	T_m	大部分外包至 CSP	—

结束语 本文提出一种多授权中心下支持属性撤销的外包解密方案。根据表 1, 与已有多授权方案相对比, 本方案在用户端有明显的存储开销优势, 访问通信开销与文献[17]方案相同的条件下用户端的解密开销相比有了大幅降低, 并且将大部分解密任务外包给云服务提供商, 当属性撤销时不需要用户参与密钥的更新操作, 降低了用户计算开销; 在用户端解密时间与文献[18]方案相同的条件下, 存储开销和访问通信量有了显著的降低, 并且用户端不参与属性的撤销计算。综上, 所提方案充分利用了云服务端的强大计算能力, 在提高系统运行效率的同时大幅降低了用户端的计算和存储成本。

参考文献

- [1] Feng Deng-guo, Zhang Min, Zhang Yan, et al. Studay 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] Lin Chuang, Su Wen-bo, Meng Kun, et al. Cloud Computing Security: Architecture, Mechanism and Modeling[J]. Chinese Journal of Computers, 2013, 9(36): 1765-1784 (in Chinese)
林闯, 苏文博, 孟坤, 等. 云计算安全: 架构、机制与模型评价[J]. 计算机学报, 2013, 9(36): 1765-1784

- [3] Hong Cheng, Zhang Min, Feng Deng-guo. Achieving efficient dynamic cryptographic access control in cloud storage[J]. Journal on Communications, 2011, 32(7): 125-132 (in Chinese)
洪澄, 张敏, 冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7): 125-132
- [4] Sahai A, Water B. Fuzzy identity-based encryption[C]//Proc of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005: 457-473
- [5] Goyal V, Pandey O, Sahai A, et al. Attribute based encryption for fine-grained access control of encrypted data[C]//Proc of ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 89-98
- [6] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Proc of IEEE Symposium on Security and Privacy. IEEE Press, 2007: 321-334
- [7] Wen Yu-hui, Chen Guang-yong, Zhao Jin-tao. Solution of data access control with ciphertext-policy attribute-based encryption in cloud computing[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2013, 25(5): 658-664 (in Chinese)

(下转第 208 页)

- [4] Sathiamoorthy M, Asteris M, Papailiopoulos D, et al. XORing elephants: Novel erasure codes for big data[C]//VLDB Endowment. Riva del Garda, Italy: dbTrento, 2013; 325-336
- [5] Rodrigues R, Liskov B. High availability in DHTs: Erasure coding vs. replication[C]//Proc of IPTPS. Ithaca, NY, USA: Springer Berlin Heidelberg, 2005; 226-239
- [6] Rashmi K V, Nakkiran P, Wang Jing-yan, et al. Having Your Cake and Eating It Too: Jointly Optimal Erasure Codes for I/O, Storage, and Network-bandwidth[C]//USENIX Conference on File and Storage Technologies. Santa Clare, CA, USA: USENIX, 2015; 81-94
- [7] Dimakis A G, Godfrey P B, Wu Yun-nan, et al. Network coding for distributed storage systems[J]. IEEE Trans on Information Theory, 2010, 56(9): 4539-4551
- [8] Ahlswede R, Cai N, Li S Y R, et al. Network information flow[J]. IEEE Trans on Information Theory, 2000, 46(4): 1204-1216
- [9] Lin S J, Chung W H. Novel Repair-by-Transfer Codes and Systematic Exact-MBR Codes with Lower Complexities and Smaller Field Sizes[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12): 3232-3241
- [10] Hu Yu-chong, Lee P, Shum K W. Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems[C]//INFOCOM. Turin, IEEE, 2013; 2355-2363
- [11] Yang Bin, Tang Xiao-hu, Li Jie. A Systematic Piggybacking Design for Minimum Storage Regenerating Codes[J]. IEEE Transactions on Information Theory, 2015, 61(11): 5779-5786
- [12] Liang Song-tao, Liang Wen-juan, Kan Hai-bin. Construction of one special minimum storage regenerating code when $\alpha=2$ [J]. Science China Information Sciences, 2015, 58(8): 1-10
- [13] Bhagwan R, Tati K, Cheng Yu-chung, et al. Total recall: System support for automated availability management[J]. Nsdi, 2004, 1: 337-350
- [14] Shvachko K, Kuang H, Radia S, et al. The Hadoop distributed file system[C]//Symp. on Mass Storage Systems and Technologies. USA: IEEE, 2010; 1-10
- [15] Bhagwan R, Savage S, Voelker G M. Understanding availability[C]//International Workshop on Peer-to-Peer Systems. Berkeley, California, USA: Springer Berlin Heidelberg, 2003; 256-257
- [16] Hwang K, Fox G C, Dongarra J J. Distributed and Cloud Computing: From Parallel Processing to the Internet of Things[M]. Morgan Kaufmann, 2011
- [17] Dimakis A G, Ramchandran K, Wu Yun-nan, et al. A Survey on network codes for distributed storage[J]. Proceeding of the IEEE, 2011, 99(3): 476-489
- [18] Rashmi K V, Shah N B, Kumar P V. Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction[J]. IEEE Transaction on Information Theory, 2011, 57(8): 5227-5239
- [19] Hu Yu-chong, Xu Yin-long, Wang Xiao-zhao, et al. Cooperative Recovery of Distributed Storage Systems from Multiple Losses with Network Coding[J]. IEEE Journal on Selected Areas in Communications, 2010, 28(2): 268-276
- [20] Kermarrec A M, Scouarnec N L, Straub G. Repairing multiple failures with coordinated and adaptive regenerating codes[C]//International Symposium on Network Coding. Beijing: IEEE, 2011; 1-6

(上接第 183 页)

- 温昱晖, 陈广勇, 赵劲涛. 基于 CP-ABE 在云计算中实现数据访问控制的方案[J]. 重庆邮电大学学报(自然科学版), 2013, 25(5): 658-664
- [8] Chase M. Multi-Authority attribute based encryption[C]//Proc of the 4th Theory of Cryptography Conf. Germany: Springer Berlin Heidelberg, 2007; 515-534
- [9] Ruj S, Nayak A, Stojmenovic I. DAC: Distributed access control in clouds[C]//Proc of the 10th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. Washington, DC: IEEE Press, 2011; 91-98
- [10] Liu Xue-jiao, Xia Ying-jie, Jiang Sha-sha, et al. Hierarchical attribute-based access control with authentication for outsourced data in cloud computing[C]//Proc of the 2013 12th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. Australia: IEEE Press, 2013; 477-484
- [11] Yang Geng, Wang Dong-yang, Zhang Ting, et al. Attribute-Based Access Control with Multi-Authority Structure in Cloud Computing[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science), 2014, 34(2): 2-9(in Chinese)
杨庚, 王东阳, 张婷, 等. 云计算环境中基于属性的多权威访问控制方法[J]. 南京邮电大学学报(自然科学), 2014, 34(2): 2-9
- [12] Huang Xiao-feng, Qi Tao, Qin Bao-dong, et al. Multi-Authority Attribute Based Encryption Scheme Revocation[C]//2015 24th International Conference on Computer Communication and Networks (ICCCN). IEEE Press, 2015; 1-5
- [13] Chen Yan-li, Song Ling-ling, Yang Geng. Attribute-based access control for multi-authority system with constant size ciphertext in cloud computing[J]. Wireless Communication Over Zigbee for Automotive Inclination Measurement China Communications, 2016, 13(2): 146-162
- [14] Xu X, Zhou J, Wang X, et al. Multi-Authority proxy re-encryption based on CPABE for cloud storage systems[J]. Journal of Systems Engineering and Electronics, 2016, 27(1): 211-223
- [15] Chen Dan-wei, Wan Liang-qing, Wang Chen, et al. A Multi-authority Attribute-Based Encryption Scheme with Pre-decryption[C]//2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP). IEEE Press, 2015; 223-228
- [16] Li Yong, Zeng Zhen-yu, Zhang Xiao-fei. Outsourced decryption scheme supporting attribute revocation[J]. Journal of Tsinghua University(Sci & Technol), 2013, 53(12): 1664-1669(in Chinese)
李勇, 曾振宇, 张晓菲. 支持属性撤销的外包解密方案[J]. 清华大学学报(自然科学版), 2013, 53(12): 1664-1669
- [17] Yang Kan, Jia Xiao-hua, Ren Kui, et al. DAC-MACS: Effective data access control for multi-authority cloud storage systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1790-1801
- [18] Rong Xing, Zhao Yong, Jiang Rong. MMACS: A Multi-Authority Cloud Access Scheme with Mixed Access Structure[C]//Proc of Workshop on Secure Networking and Forensic Computing. Sydney, NSW: IEEE Press, 2014; 706-711