基于隐秘映射组合公钥的云计算密钥管理方案*

宋宁宁, 刘蕴络, 姚倩燕, 刘 倩
(北京科技大学 计算机与通信工程学院, 北京 100083)

摘 要: 为了保证云计算安全,在分析云计算的安全需求的基础上,基于椭圆曲线密码体制提出了一种适用于分布式云计算的隐秘映射组合公钥密钥管理方案。详细地阐述了密钥管理的一系列操作过程,包括密钥初始化、密钥分发、密钥协商、密钥更新及密钥销毁等。分析表明,该方案能够正确高效地解决云计算密钥大规模管理和存储问题,具有高度可扩展性,能够抵抗共谋攻击,能保证云计算提供安全可靠的服务。

关键词: 云计算; 椭圆曲线; 组合公钥; 密钥管理; 隐秘映射
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2013)09-2759-04
doi:10.3969/j.issn.1001-3695.2013.09.050

Cloud computing key management scheme based on covert mapping combined public key

SONG Ning-ning, LIU Yun-luo, YAO Qian-yan, LIU Qian
(*School of Computer & Communication Engineering*, *University of Science & Technology Beijing*, *Beijing* 100083, *China*)

Abstract: In order to guarantee the security of cloud computing, based on the analysis of cloud computing security requirements and elliptic curve cryptosystems, this paper proposed a covert mapping combined public key management scheme that was suitable for the distributed cloud computing. It made detailed description of the process of key management, such as key initialization, key distribution, key agreement, key update and key revocation. The analysis results show that the scheme can solve the problem of large scale keys storage and management correctly and efficiently, has high scalability, can resist collusion attack and ensur the security services provided by cloud computing.

Key words: cloud computing; elliptic curve; combined public key; key management; covert mapping

0 引言

云计算是一种虚拟资源池,是一种按需付费的模式,通过虚拟机的运行实现动态地重构以满足用户的需求。云计算具有许多优点,例如快速的部署、较低的费用、可扩展性、快速的供应、高弹性、泛在网络的接入、应对攻击时的系统管理保护、实时检测系统窜改以及快速的服务重建等[1]。基于计算资源基础设施的云,它是通过动态地按需产生和撤销虚拟机节点,动态可扩展地为用户提供基于虚拟架构的按需付费服务。它容许虚拟机服务器按需地增加和减少,以减小云中资源的占用和消耗。云计算的这种可扩展性使它能够提供一种理想化的大规模基础架构,同时这也产生了一系列安全隐患,包括数据安全、虚拟机安全、软件安全等[2]。然而,传统的安全保护手段并不足以保证大规模云计算使用过程中的安全,特别是大规模密钥的安全和管理问题。文献[3]介绍了一种利用 PKI 证书保护云环境中加密密钥申请的方案,对称密钥通过证书中的公钥加密进行存储;但证书的私钥不易于记忆,用户需要随身携带私钥。文献[4]将密钥与文件进行绑定存储,便于密钥的管理更新与维护,但该方案只适用于云中存储数据文件时的密钥管理,具有局限性。而且这些密钥管理方案都没有解决规模化的问题。

大规模是云计算的首要特征,只有大规模的云计算才能实现云计算各种服务优势,尤其是服务的能力和服务规模经济。组合公钥(CPK)[5]是基于矩阵元素组合的公钥体制,将密钥生产和密钥管理结合起来,以很少的密钥矩阵存储量满足密钥的大规模需求。但是,由于组合公钥技术中公私钥的生成是由公私钥矩阵元素的线性组合构成,在满足一定的条件下,存在用部分私钥额可以计算出整个私钥矩阵的共谋安全威胁,主要包括线性分析共谋攻击[6]、选择性共谋攻击[7]和随机共谋攻击[7]。文献[8,9]采用硬件加密手段对用户私钥进行保护,进而防止共谋攻击。由于私钥采用物理手段加以保护,这使得密钥更新变得困难。文献[10~12]通过随机密钥的方式来消除用户之间私钥的线性关系,从而抵抗共谋攻击。当网络规模较大时,随机密钥的管理问题难以解决。文献[13,14]采用基于双矩阵的组合公钥技术,能在保持组合公钥体制优点的基础上对抗选择性共谋攻击和随机共谋攻击。但是基于双矩阵的机制中求解非线性方程组可以转换为求解线性方程组,因此仍然存在线性分析共谋攻击问题[13]。

本文在分析了云计算特点的基础上,提出了一种适用于云

收稿日期: 2012-11-30; **修回日期**: 2013-03-04 **基金项目**: 国家教育部重大基金资助项目(311007);国家自然科学基金资助项目(61170014)

作者简介:宋宁宁(1987-),男,山东临沂人,博士研究生,主要研究方向为云计算、网络安全(6221294@163.com);刘蕴络(1963-),女,硕士,主要研究方向为电子电路;姚倩燕(1987-),女,福建福州人,硕士研究生,主要研究方向为云计算、网络安全;刘倩(1987-),女,河南郑州人,博士研究生,主要研究方向为网络安全路由.

计算的基于隐秘映射组合公钥技术(covert mapping combined public key,CM-CPK)的密钥管理方案,对云中的密钥进行统一的生成、分发、更新等。CM-CPK 是一种集中式的密码技术,利用该技术实现的密钥管理方案,只需要少量的种子就可以生成海量的公私密钥对,这种特征使其非常适用于云计算环境,以解决大规模密钥管理的问题。本方案采用的隐秘映射机制,对公钥矩阵计算公钥的过程进行保护,使恶意用户无法构造推算密钥矩阵的线性方程组,达到对抗共谋攻击的目的;而且它的破解难度更大,资源消耗更小。

1 系统总体结构

本文构建了一个基于隐秘映射组合公钥的云计算密钥管理架构,如图 1 所示。

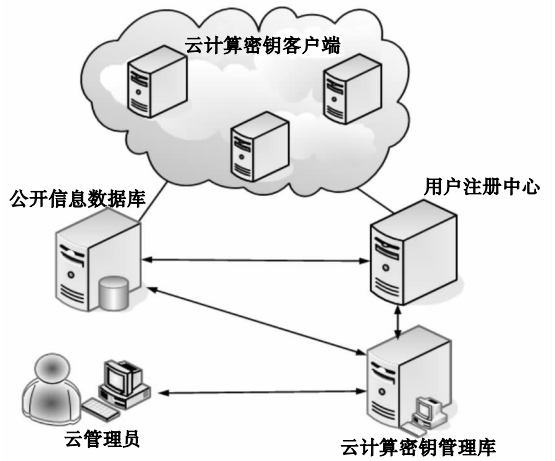

图1 云安全CPK密钥管理系统总体结构

当有新密钥客户端节点要加入到云环境中时,它需要跟云计算密钥管理系统中的各个组件进行信息的交互,以获取节点的私钥。该系统主要包括以下几个组件:

a)云计算密钥管理中心。负责系统的初始化,椭圆曲线的产生、公私钥因子矩阵的组合和公私密钥对的生成及管理。

b)用户注册中心。负责用户的注册审核,并向公开信息数据库发放用户的有效及废弃的身份信息,同时还负责向云计算密钥管理中心转发注册用户的私钥发放申请。

c)公开信息数据库。保存用户有效的及废弃的身份信息,同时存储公钥因子矩阵列表。

d)云计算密钥客户端。使用云计算服务的企业或者个人用户,向注册中心发起注册和私钥发放申请。

e)云管理员。云计算服务提供商,负责管理和维护整个云计算密钥管理系统。

2 系统功能模块设计

2.1 系统初始化

云计算隐秘映射组合公钥密钥管理是基于椭圆曲线密码体制的,它的安全性建立在椭圆曲线离散对数难题上[5]。假设一个有限域 F 的特征 p 是素数,且 p 不等于 2 或 3,$P=(x_P, y_P)$ 是椭圆曲线的基点。可将椭圆曲线 E_F 定义[5]为

$$y^2 = x^3 + ax + b \quad a,b \in F \tag{1}$$

设椭圆曲线的参数组为(a,b,P,n,p),P 的子群 M 可以表示成$\{P,2P,3P,\cdots,(n-1)P,nP\}$,可以从子群 M 中得出这样的等式:$R_{ij}=s_{ij}P$。私钥因子矩阵 SSK 由元素 s_{ij}组成,公钥因子矩阵 PSK 由元素 R_{ij}组成,这两个矩阵就可以分别定义为

$$\mathrm{SSK}=\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1j} \\ s_{21} & s_{22} & \cdots & s_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ s_{i1} & s_{i2} & \cdots & s_{ij} \end{bmatrix},\ \mathrm{PSK}=\begin{bmatrix} R_{11} & R_{12} & \cdots & R_{1j} \\ R_{21} & R_{22} & \cdots & R_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ R_{i1} & R_{i2} & \cdots & R_{ij} \end{bmatrix} \tag{2}$$

在 CPK 密码体制中,公私钥对是通过指向公私钥因子矩阵对应位置上的元素的组合而产生的。可以利用哈希函数和行映射算法以及列置换算法[5]实现标志到因子矩阵坐标的映射,以选出因子矩阵中的元素,具体的算法实现流程如图 2 所示。

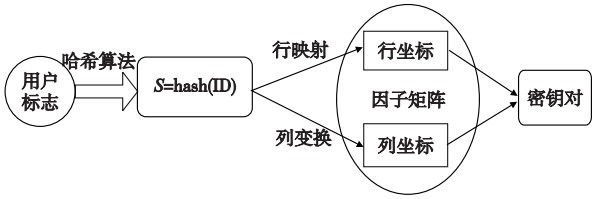

图2 组合公钥中标志映射算法的实现

根据行映射和列置换得出的随机序列向量,分别为$(i_1,i_2,\cdots,i_j)$和$(j_1,j_2,\cdots,j_j)$,取出私钥因子矩阵中对应的各个元素因子相加,即可得出用户的私钥为

$$sk=(s_{i_1,j_1}+s_{i_2,j_2}+\cdots+s_{ij,jj}) \bmod n \tag{3}$$

同样,选取出公钥因子矩阵的元素因子,进行点加运算,组合出对应的用户公钥:

$$pk=R_{i_1,j_1}+R_{i_2,j_2}+\cdots+R_{ij,jj}= s_{i_1,j_1}P+s_{i_2,j_2}P+\cdots+s_{ij,jj}P \tag{4}$$

云计算组合公钥密钥管理系统中的 pk 与 sk 构成一对公私钥。从式(3)和(4)可以看出,公钥 pk 正好是私钥 sk 关于基点 P 的倍数。

本方案采用隐秘映射机制,云计算密钥管理中心将密钥映射及矩阵变换采用物理保护的方式写入云计算客户端的硬件中,并采用加密手段,使得客户端只能使用该隐秘映射模块,但不能获取内部具体的流程和中间参数,比如根据行映射和列置换得出的随机序列向量等。算法流程如图 3 所示。

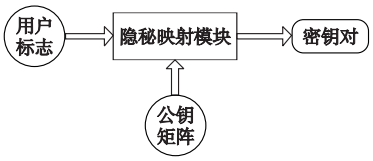

图3 隐秘映射机制

2.2 密钥分发

云计算组合公钥密钥管理系统中的密钥分发涉及到系统中的多个组件,主要包括:

a)公钥因子矩阵。云计算密钥管理中心生成公钥因子矩阵后,发送给公开信息数据库保存。该数据库开放给所有用户,任何其他用户都可以通过访问该公开信息数据库以获取公钥因子矩阵。

b)私钥因子矩阵。私钥因子矩阵也是由云计算密钥管理中心生成,然后就始终存储于该密钥管理中心。在系统的整个密钥产生和分发的过程中,私钥因子矩阵都是要严格保密的。

c)公钥。由云计算密钥管理中心通过用户标志映射以及组合公钥因子矩阵产生。本方案采用隐秘映射机制,客户端用户根据用户标志和公钥矩阵,通过隐秘映射模块可以计算出需

要的公钥。由于硬件物理保护,计算的中间过程及中间参数(如根据行映射和列置换得出的随机序列向量等)对客户端用户保密。

d)私钥。用户通过用户注册中心向云计算密钥管理中心申请私钥。云计算密钥管理中心生成私钥后,通过安全信道向用户注册中心发放私钥,而用户注册中心则将私钥写入安全存储介质交给用户。

2.3　密钥协商

若云环境中有两个用户需要进行通信,那么它们必须采用组合公钥技术进行密钥协商,以获取只有双方知道的相同的会话密钥。

设云中的用户 A 和用户 B 的标志分别为 ID_A、ID_B,k_{AB}表示用户 A 与用户 B 之间的会话密钥;$\mathrm{ECC}_k(m)$表示利用密钥 k 对消息 m 进行椭圆曲线加/解密和签名[1],$\mathrm{AES}_k(m)$表示利用密钥 k 对消息 m 进行 AES 对称加解密;符号"‖"表示消息的级联。则具体的密钥协商过程如图 4 所示。

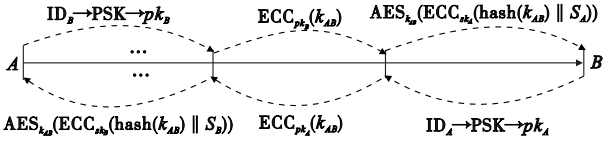

图4　用户A与用户B的密钥协商

用户 A 和用户 B 都已经拥有了它们各自的私钥 sk_A 和 sk_B,并且共同保存同一个随机序列码。当用户 A 将消息包 $\mathrm{ECC}_{pk_B}(k_{AB})$和 $\mathrm{AES}_{k_{AB}}(\mathrm{ECC}_{sk_A}(\mathrm{hash}(k_{AB}) \| S_A))$发送给用户 B 后,用户 B 可以利用自己的私钥 sk_B 对消息包 $\mathrm{ECC}_{pk_B}(k_{AB})$进行解密,获取由 A 生成的会话密钥 k_{AB};然后继续利用该会话密钥解密消息包 $\mathrm{AES}_{k_{AB}}(\mathrm{ECC}_{sk_A}(\mathrm{hash}(k_{AB}) \| S_A))$,获取消息包 $\mathrm{ECC}_{sk_A}(\mathrm{hash}(k_{AB}) \| S_A)$。

由于云密钥管理系统中所有用户的身份标志以及公钥因子矩阵都可以在系统的公开信息数据库中查询到,因此,用户 A 和用户 B 的这两项信息对双方都是已知的。借助隐秘映射模块,利用公钥因子矩阵可以进一步获得对方的公钥。

如果用户 B 利用自己计算出的用户 A 的公钥 pk_A 成功地验证了消息包 $\mathrm{ECC}_{sk_A}(\mathrm{hash}(k_{AB}) \| S_A)$中的 ECC 签名,就证明了发送消息包的用户 A 的身份是正确的。

签名验证成功后,用户 B 就得到了用户 A 的随机序列码 S_A。如果用户 B 获取的随机序列码 S_A 与自身保存的随机序列码 S_B 相同,那么这个消息包就是新鲜的,从而保证密钥协商过程能够抵御重放攻击。

签名验证成功后,用户 B 同时也得到了 k_{AB}的哈希值 hash(k_{AB}),而用户 B 在解密消息包时就得到了会话密钥 k_{AB},这时,同样计算 k_{AB}的哈希值 hash2(k_{AB}),比较 hash(k_{AB})和 hash2(k_{AB}),如果它们是相等的,则保证了消息的完整性。

2.4　密钥更新

随着密钥使用次数的增加,密钥的安全性降低。此外,随着系统中用户的撤销及加入,密钥矩阵也面临密钥资料枯竭的问题。本方案的密钥更新包括两部分。

1)用户密钥对的更新　当用户 A 需要进行密钥更新时,向云计算密钥管理中心提交更新请求,并验证存放在用户注册中心中的身份标志是否有效。若验证通过,密钥管理中心存储该节点身份标志到废弃标志库,并为用户 A 分配新的身份标志,更新用户注册中心中存放的旧的标志。云计算密钥管理中心则利用新的身份标志重新计算私钥,然后将用户 A 的新私钥及新的身份标志发送给用户 A,同时将新标志存入公开信息数据库,并在系统内进行广播。具体的密钥更新过程如图 5 所示。

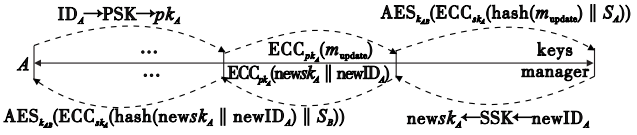

图5　用户A的密钥更新过程

2)密钥矩阵的更新　云计算密钥管理中心根据系统需求指定整个系统密钥统一更新的时间,到了指定的更新时间,更新整个公私钥矩阵,并将公钥矩阵及用户私钥分发到各个用户中。分发过程的安全由用户的原有密钥进行保证,具体更新过程略。

2.5　用户的加入和退出

1)用户的加入　当系统中有新用户加入时,云计算密钥管理中心为该节点配置对应的参数信息,包括密钥初始化中的各种参数,用户标志 ID,进而生成新用户的公私钥对;并通过安全信道将用户标志 ID、公私钥对分发给用户,具体流程略。

2)用户的退出　当有节点退出系统时,它向云计算密钥管理中心发出退出请求,密钥管理中心存储该节点身份标志到废弃标志库,防止以后再次将此身份标志分配给其他用户,保证系统的安全性,具体流程略。

3　方案安全及性能分析

通过以上方案的详细设计过程可以看出基于隐秘映射组合公钥技术的密钥管理方案不仅能够满足大规模密钥管理的需求,能很好地保证系统的安全,并且具有较高的性能。下面对方案的安全性和性能进行具体的分析。

1)安全性分析

(1)加密机制安全性分析

本文提出的密钥管理方案是建立在椭圆曲线离散对数难题上,因此产生的密钥是安全的。每个发送和接收的信息包都是加密的,可以对抗攻击者的截获偷听。关于椭圆曲线离散对数的安全性分析,在这里不再详述。

(2)前向安全和后向安全分析

对每个客户端分配唯一的身份标志,任何两个节点拥有不同的公私钥对,可以保证节点的私钥是安全保密的。当系统中有新用户加入时,云计算密钥管理中心为其分配未使用过的身份标志,并通过安全方式将私钥和身份标志发送给用户。新用户无法获得之前用户的私钥,因此可以保证前向安全。当系统由用户退出时,云计算密钥管理中心将该用户的身份标志存入废弃标志库,以后不再使用,因此可以保证系统后向安全。

(3)数据完整性分析

在密钥协商、密钥更新等过程中,对敏感数据采用哈希运算得到其哈希值,将哈希值连同哈希值的加密结果以及加密的敏感信息发送给对方。当数据包被恶意窜改后,通过再次计算哈希值跟解密后的哈希值进行比对,可以发现恶意窜改攻击,从而保证数据的完整性。

(4)抵御重放攻击分析

在每一次发送的数据包中添加随机序列码,并通过上述方

式保证其完整性。在签名验证成功后,用户通过比对随机序列码可以判定某个消息包是否是新鲜的,从而保证密钥协商过程能够抵御重放攻击。

(5)抵御共谋攻击分析

针对抵抗共谋攻击,由组合公钥的原理可知,用户的私钥是私钥矩阵和随机序列向量的线性组合。在以往的组合公钥方案中,用户输入用户标志,经过映射算法得到随机序列向量,然后由公钥矩阵和随机序列向量计算出公钥。映射算法和随机序列向量都是公开的。由于公钥矩阵和私钥矩阵存在一对一的关系,因此共谋攻击者根据随机序列向量(即系数矩阵)和私钥(即常数列)可以构建线性方程组,获得全部组合私钥矩阵,进而破解整个 CPK 系统。

在本方案中,采用隐秘映射机制将密钥映射及矩阵变换采用物理保护的方式,使用户只能使用映射算法和随机序列向量,而不能获取具体的过程和参数。共谋攻击者无法获得随机序列向量,即线性方程组中的系数矩阵,因此无法构建线性方程组对私钥矩阵进行破解,从而达到抵抗共谋攻击的目的。

2)性能分析

(1)存储开销

在计算 CPK 密钥管理系统中,用户只负责存储用户私钥以及公钥因子矩阵,而当公钥因子矩阵的大小为 $p \times q$ 时,它可以组合出 p^q 对的公钥,却只需要 $p \times q$ 的存储量。该系统仅占用少量的存储空间,就实现了云计算大规模的密钥存储。

(2)可扩展性

该系统中,$p \times q$ 大小的公私钥因子矩阵就可以组合生成 p^q 密钥量的公私钥对。例如,如果公钥的大小是 192 bit,则 50 KB 大小的公钥因子矩阵可以组合出估计 10^{48} 密钥量的公钥对。由数量有限的矩阵因子组合出如此庞大的公私钥对,极大地增强了系统的可扩展性。

(3)复杂性

该系统集中生成密钥、将密钥分散存储,并通过映射算法将用户的标志组合成实体的公钥,密钥的管理就简化成了用户标志的管理。这些方式都大大减小了云计算中大规模密钥管理的复杂性。

4 仿真实验

本文利用 CloudSim 云计算模拟工具[15],对所设计的云计算隐秘组合密钥管理系统进行仿真,以实验说明密钥管理过程中椭圆曲线的安全产生、公私密钥对的生成等过程,验证云安全 CPK 密钥管理方案的可行性与安全性。

CloudSim 只支持云计算的资源调度和管理服务等的建模,本文必须对该仿真平台进行扩展以模拟密钥生成过程。编写 Java 代码在 My eclipse 上重新编译,生成的安全椭圆曲线和公私密钥对如图 6 所示。验证了云计算隐秘映射组合公钥密钥管理系统中的密钥生成可行性。

5 结束语

本文设计了云计算隐秘映射组合公钥密钥管理方案,并实现了云计算密钥管理的一系列密钥操作,包括密钥生成、分发、协商等,所设计的方案能够满足云计算大规模密钥管理的要求,并且具有高度的可扩展性,可以抵抗共谋攻击。最后还在云仿真平台上,测试了密钥管理系统中公私密钥对的生成功能。若将角色分离访问控制的思想与本文的方案相结合,对使用密钥的不同可信等级实体进行限制,可以进一步加强云计算环境的安全性,这可以成为以后的研究方向。

图6 产生椭圆曲线和公私密钥对的仿真

参考文献:

[1] SUBASGINI S, AVITHA V. A survey on security issues in service delivery models of cloud computing[J]. Journal of Network and Computer Applications,2011,34(1):1-11.

[2] BEHL A, BEHL K. An analysis of cloud computing security issues [C]//Proc of World Congress on Information and Communication Technologies. [S. l.]:IEEE Press,2012:109-114.

[3] SUN Lei, DAI Zi-shan, GUO Jin-di. Research on key management infrastructure in cloud computing environment[C]//Proc of the 9th International Conference on Grid and Cooperative Computing. Washington DC:IEEE Computer Society,2010:404-407.

[4] 陈富汉,柳毅,余琦. 面向个人云计算的数据存储密钥管理方案[J]. 现代计算机, 2011(12):8-10.

[5] 南相浩. CPK 组合公钥体制(v7.0)[J]. 计算机安全,2012(5):2-4.

[6] 陈华平,关志. 关于 CPK 若干问题的说明[J]. 信息安全域通信保密,2007(9):47-49.

[7] 赵美玲, 张少武. 基于 ECC 的组合公钥技术的安全性分析[J]. 计算机工程, 2008,34(1):156-157.

[8] 南湘浩. CPK 标识认证[M]. 北京: 国防工业出版社,2006:50-60.

[9] 余彦峰,刘毅,张书杰,等. 一种专用可信网络[J]. 北京工业大学学报, 2006,32(11): 1032-1036.

[10] 南湘浩,陈华平. 组合公钥(CPK)体制标准[J]. 信息安全与通信保密,2008(8):21-22.

[11] 陈文华,肖亦伟. 基于 CPK 的 IBE 方案[J]. 软件导刊, 2008,7(2): 88-89.

[12] 徐鹏,崔国华,雷凤宇. 非双线性映射下一种实用的和可证明安全的 IBE 方案[J]. 计算机研究与发展,2008,45(10):1687-1695.

[13] 邵春雨,苏锦海,魏有国,等. 一种双矩阵组合公钥算法[J]. 电子学报,2011,39(3):671-674.

[14] 龙弟强,王亚弟,韩继红,等. 一种基于双矩阵组合公钥算法的密钥生成方案[J]. 计算机应用研究,2011,28(8):3058-3060.

[15] CALGEIROS R N, RANJAN R, BELOGLAZOV A, *et al*. CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms[J]. Software: Practice and Experience,2011,41(1):23-50.