基于 AES 和 ECC 的云审计数据加密方案

陈 庄 叶成荫
(重庆理工大学计算机科学与工程学院 重庆 400054)

摘 要 针对云审计数据的单向加密所带来的数据传输及存储安全问题,提出了混合双向加密方案(Hybrid Bidirectional Encryption Scheme,HBES)。HBES 私钥由事件发起者产生并本地化存储,其中,私钥由随机数通过映射规则得到,随机数的产生则由响应时间和外部因素决定。模拟实验结果表明:与单一加密方式相比,HBES 在加密时间开销以及安全方面更加高效,在实现云端审计数据的加解密方面是切实可行的。

关键词 AES,ECC,云审计,双向加密
中图法分类号 TP309 **文献标识码** A

Scheme of Cloud Audit Data Encryption Based on AES and ECC

CHEN Zhuang YE Cheng-yin
(College of Computer Science and Engineering,Chongqing University of Technology,Chongqing 400054,China)

Abstract Focusing on the data transmission and storage security problem of one-way encryption of cloud audit data, HBES (Hybrid Bidirectional Encryption Scheme) was proposed to tackle this problem. HBES private key is brought by event sponsor and local storage, then random number which depends on response time and external factors generates private key by mapping rules. Corresponding simulation experiment advocates that compared with the one-way encryption method, HBES is a more effective and feasible way in encryption time, security and achieving the encryption and decryption of the cloud audit data.

Keywords AES,ECC,Cloud audit,Bidirectional encryption

1 引言

随着基于互联网虚拟化资源云计算平台的成熟,将该平台广泛地应用于审计工作将引发审计业新的发展趋势。云审计使审计人员可以方便地使用存储在云端的数据,不仅节约了审计时间,提高了效率,而且打破了地点限制,促进了审计任意性。然而,云审计在给审计发展带来机遇的同时,也带来了前所未有的挑战[1],用户数据存储在云端,远离了用户可控范围,使数据面临着存储及传输安全问题。根据 Twin Strata 公司的调查结果:约有 20%的人愿意使用云端存储数据,仅有不到 50%的人愿意使用云存储进行数据备份、归档等作业。而在我国约有 85%的公司由于数据安全性而不敢将数据放在公共云上。在 2016 年 RSA 大会上云计算安全和安全云被指出依然是热点问题,而将云计算应用于审计领域最大的挑战仍然是云的安全问题。目前,我国云审计平台正处于加快建设阶段,保障云端存储及传输过程中数据的安全性也显得尤为重要[2-4]。将加密技术应用于云审计平台是一种常见的保护数据安全性的有效方法[5],但目前大多数的加密方案为单向数据加密,即接收方收到加密数据后进行解密得到明文,并进行本地化存储,而无需再向发送方发送明文数据,形成双向数据交互,从而无法满足云审计要求的双向数据传输,形成数据双向审计交互的壁垒。目前,我国在主流云平台可采取 Cloudfogger 对存储数据进行 256 位 AES 加密[6],若在云审计方面采用 CloudfoggerAES-256 对审计数据进行加密,客户端、云端以及审计端之间会频繁地在网络上出现私钥的传输,这不利于数据的安全性传输及存储。基于此,本文提出了混合双向加密方案 HBES(Hybrid Bidirectional Encryption Scheme),即在云审计领域利用 AES 加密数据并结合 ECC 加密传送公钥的方法在上传、下载数据时对数据进行双向加密,使得每次作为数据的接收方产生并保存 ECC 私钥,而在网络中传送的只有公钥。这样即使被窃取了传输数据和公钥,但由于私钥的本地化存储,没有办法获取私钥解密,从而无法获取明文,继而保障数据传输的安全性和加密的高效性。

2 相关工作

A. Kerkhoff 等[7]曾提出了被称为 Kerkhoff 原理的基础假设,为解决数据加密安全性问题提供了思路,引起了学术界的普遍关注。即假设窃取者知道加密算法原理及实现过程,那么就认为加密系统的安全性完全依赖于密钥的安全性。基于此,要求更加注重对密钥安全性的保护。如果可以进一步对密钥进行相应的加密,可以在一定程度上达到保护密钥,进而保护数据安全性的目的。因此,混合加密算法应运而生。混合加密算法是指用密钥 k 对数据加密后,再对 k 进行一次

本文受重庆市研究生科研创新项目(CYS16222),重庆理工大学研究生创新基金(YCX2015222,YCX2015237,YCX2016229)资助。
陈 庄(1964-),男,博士,教授,主要研究方向为企业信息化管理、网络与信息安全等,E-mail:13608377531@139.com;叶成荫(1990-),男,硕士生,主要研究方向为网络与信息安全、应用密码学。

加密，从而达到保护密钥及数据安全性的目的。随着云计算的发展，将混合加密算法应用到云计算中保证云端数据安全在近年来也有了相应的研究。洪澄等[8]针对云存储中保护敏感数据问题，在基于属性加密的基础上提出了 Hybrid Cloud Re-Encryption（HCRE），该方法旨在从访问控制角度出发保证云数据安全。TEBAA Maha 等[9]提出在云计算系统中使用同态加密算法保障云数据的安全性。文献[10]考虑采取动态生成 DES 密钥结合 RSA 加密算法对云数据进行二次加密，保障数据传输过程中的安全性。文献[11]讨论了在电子商务领域使用 ECC 和 AES 相结合的加密方案，实现加密效率更高、安全性更好的加密系统。文献[12]也阐述了混合加密算法安全的可证明性。

然而以上方案只应用于云计算平台，在云审计领域，由于云审计要求数据在云端以密文形式存储，而在客户端或审计端则需要数据以明文形式上传或审计，因此若采取以上方案，则私钥会频繁分发，增加了在网络传输中被非法窃取的可能性，不利于审计数据的安全性。

基于此，本文在混合加密算法 HEA（Hybrid Encryption Algorithm）的基础上提出了混合双向加密方案 HBES（Hybrid Bidirectional Encryption Scheme），即在云审计领域利用 AES 加密数据并结合 ECC 加密传送公钥的方法在上传、下载数据时对数据进行双向加密，使私钥本地化存储。作为数据的接收方产生并保存 ECC 私钥 k，通过 $K=kG$，得到公钥 K 并用 K 去加密发送方已有的私钥 k_1，再将已加密的 k_1 和数据发送给接收端。这样不仅将 HEA 应用在了云审计领域，也摒弃了频繁的私钥分发，在保持审计数据高效加解密的前提下，保证了数据的安全性。

3 混合双向加密方案

基于对称加密算法 AES 和非对称加密算法 ECC 的优缺点，本文提出了将两者相结合的混合双向加密方案（HBES），在由企业上传审计数据到云端和审计人员从云端下载审计数据时，使用 AES 对称加密算法对审计数据加密，同时使用 ECC 非对称加密算法来传送 AES 的密钥，实现在上传或下载数据时只有公钥在网络中传送，而私钥保存在接收端。这样就可以在发挥 AES 和 ECC 优点的同时规避它们的缺点，实现审计数据的安全高效传输。

3.1 客户端上传数据加密方案

企业作为客户端连接互联网，通过终端设备将待审计数据加密传送至云端，上传数据加密方案流程如图 1 所示。

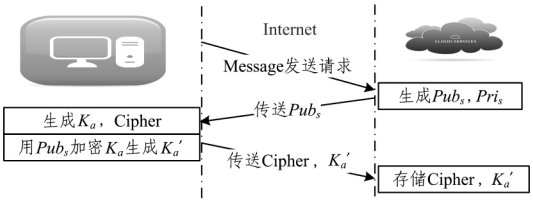

图 1 HBES 上传数据加密方案

3.1.1 客户端上传数据加密方案

总体流程为企业作为客户端向云端发送待审计数据（Message）上传请求，云端收到请求后，使用 ECC 加密算法生成私钥（Pri_s）和公钥 Pub_s），云端保留 Pri_s 并将 Pub_s 传送给客户端，同时，客户端使用 AES 加密算法生成密钥（K_a）并对 Message 加密得到密文（Cipher）。客户端在收到 Pub_s 后，用 Pub_s 对 K_a 进行加密得到 K_a' 后向云端传送 Cipher 和 K_a'。待云端接收后，以密文形式存储该信息。

3.1.2 云端私钥生成

当客户端向云端发送 Message 请求时，云端记录响应请求时间 T_r，通过 $Srand()$ 函数产生随机数种子 Z_r，得到 $M_r=rand(Z_rX)$，其中 X 为外因素，如云端的序列号等；然后进行 $M_r\%62$ 操作（产生的私钥是由 0 到 9、a 到 z 以及 A 到 Z 随机组成的 62 个字符），得到 $x\in[0,61]$ 的任意整数，以此循环得到 20 位数字（云端采用 160bit 私钥输入）；最后，构造映射表 S_r，其是由 62 位包含大小写字母及数字组成的随机排列字母表，我们定义云端产生的映射表进行横向映射转换。通过产生的 20 位随机数映射到表 S_r，产生 20 字节的由大小写字母及数字组成的私钥 Pri_s。

通过椭圆曲线计算公式，由私钥 Pri_s 计算可得到公钥 Pub_s。

3.1.3 客户端密钥的生成

当云端向客户端发送公钥时，客户端记录发送时间 T_s，通过 $Srand()$ 函数产生随机数种子 Z_s，得到 $M_s=rand(Z_sX)$，其中 X 为外因素，如客户端的 P/N 等；然后，进行 $M_s\%62$ 操作（产生的私钥是由 0 到 9、a 到 z 以及 A 到 Z 随机组成的 62 个字符），得到 $x\in[0,61]$ 的任意整数，以此循环得到 16 位数字（客户端采用 128bit 密钥输入）；最后，构造映射表 S_s，其是由 62 位包含大小写字母及数字组成的随机排列字母表，定义客户端产生的映射表进行纵向映射转换，通过产生的 16 位随机数映射到表 S_s，产生 16 字节的由大小写字母及数字组成的密钥 K_a。

3.1.4 云端存储数据方案

云端存储数据采取分布式的文件系统，云端在响应请求后生成的私钥 Pri_s 和之后由客户端传送过来的密文 Cipher 及加密后的密钥 K_a' 将存储在不同的服务器上。

3.2 审计端下载数据加密方案

待审计数据以密文形式分布式存储在云端，审计人员可通过终端设备连接互联网下载待审计数据。下载数据加密方案的流程如图 2 所示。

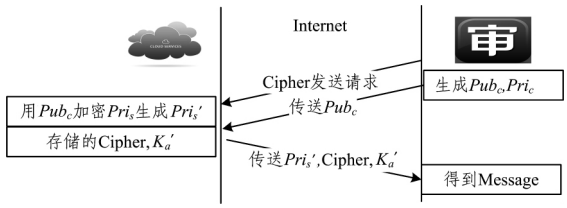

图 2 HBES 下载数据加密方案

3.2.1 审计端下载数据加密方案

审计方作为客户端向云端发送下载待审计数据（Cipher）请求，同时使用 ECC 加密算法生成公钥（Pub_c）和私钥（Pri_c），客户端保留 Pri_c 并将 Pub_c 传送给云端。云端通过 Pri_c 加密之前生成的私钥（Pri_s）得到 Pri_s'；然后将 Pri_s' 和存储在云端的 Cipher，K_a' 传送给客户端，客户端通过 Pri_c 解密 Pri_s' 得到 Pri_s；再用 Pri_s 解密 K_a' 得到 K_a；最后用 K_a 解密 Cipher 得到 Message。

3.2.2 客户端私钥生成

当审计方需对云端数据进行审计时，作为客户端记录当前时间 T_c，并通过 $Srand()$ 函数产生随机数种子 Z_c，得到 $M_c=$

$rand(Z_c X)$，其中 X 为外因素，如审计人员编号等；然后，进行 M_c%62 操作（产生的私钥是由 0 到 9、a 到 z 以及 A 到 Z 随机组成的 62 个字符），得到 $x\in[0,61]$的任意整数，以此循环得到 20 位数字（客户端采用 160bit 私钥输入）；最后，构造映射表 S_c，其是由 62 位包含大小写字母及数字组成的随机排列字母表，并通过产生的 20 位随机数纵向映射到表 S_c，产生 20 字节的由大小写字母及数字组成的私钥 Pri_c。

通过椭圆曲线计算公式由私钥 Pri_c 计算可得到公钥 Pub_c。

4　实验验证及性能分析

针对提出的混合双向加密方案，我们利用中科曙光天阔 A440-G 服务器模拟云端，并架设多台 Windows 系统主机作为客户端和审计端并与服务器连通，同时在服务器和主机上利用 VS2013 平台编写 AES、ECC 和响应请求代码，部署图如图 3 所示。在网络传输过程中部署网络损伤仪，以在实验室环境下更准确地模拟实际云传输过程中的网络延迟。

图 3　模拟实验部署图

该实验以某材料公司的盈利能力报表为测试数据，图 4 为部分实验测试数据。

利润表逼近分析

被审计单位：XX　　编制人：XX　　日期：2011年1月10日　　索引号：A_09　　索引号：A-09

会计期间或截止日：2010年12月31日　　复核人：XX　　日期：2011年1月11日　　页 码：1

项目名称	行次	本月发生数	本年累计数	结构比重	上年同期	差异额	差异率
1	2	3	4	5	6	7=4-6	B=7/6
一、营业收入	1	710,020.00	9,432,580.00	100.00%		9,432,580.00	
减：营业成本	2	355,425.95	3,833,347.99	40.64%		3,833,347.99	
营业税金及附	3	8,799.36	121,932.60	1.29%		121,932.60	
销售费用	4	12,654.37	132,522.28	1.40%		132,522.28	
管理费用	5	354,308.64	3,317,816.27	35.17%		3,317,816.27	
财务费用	6	25,034.57	18,766.25	0.20%		18,766.25	
资产减值损失	7						
加：公允价值变动收益	8						
投资收益	9		38,960.00	0.41%		38,960.00	
其中：对联营企业和合营	10						
二、营业利润	11	-46,402.89	2,047,154.61	21.70%		2,047,154.61	
加：营业外收入	12	1,289.70	9,899.48	0.10%		9,899.48	
减：营业外支出	13		6,180.00	0.07%		6,180.00	
其中：非流动资产处置损	14						
三、利润总额	15	-45,113.19	2,050,874.09	21.74%		2,050,874.09	
减：所得税费用	16		691,675.79	7.33%		691,675.79	
四、净利润	19	-45,113.19	1,359,198.30	14.41%		1,359,198.30	

图 4　某公司利润表逼近分析

4.1　实验验证

4.1.1　客户端上传数据加密实验

主机模拟客户端发送 Message 请求时，服务器记录响应请求时间戳，产生随机数种子 Z_r，得到 $M_r=rand(Z_r X)$，其中 X 为服务器序列号 9800028300376250。M_r 对 62 进行取模运算后得到表 1 所列的 20 位随机数字。

表 1　服务器产生的随机数字

17	25	52	11	15	37	7	32	4	2
54	36	14	29	45	30	3	44	39	25

服务器构建映射表 S_r，其是由 62 位包含大小写字母及数字组成的随机排列字母表，如表 2 所列。

表 2　S_r 映射表

F	1	p	f	H	p	x	x	L	I	r	v	W	6	Y	G
Z	w	Q	t	D	Y	S	X	T	T	1	H	h	c	g	g
Z	7	P	W	x	z	P	R	A	r	z	q	m	1	n	Y
n	k	3	Z	Q	b	2	m	m	F	f	U	r	f		

将表 1 产生的随机数在 S_r 映射表中进行横向映射，得到私钥 Pri_s=ZTZrYxxgf1bW6cmcpqPT。由私钥 Pri_s 计算可得到公钥 Pub_s，封装在文件中传送给主机。

主机端记录云端发送公钥的时间戳产生随机数种子 Z_s，得到 $M_s=rand(Z_s X)$，其中 X 为主机 S/N 号 WB01848026。M_s 对 62 进行取模运算得到 16 位随机数字，并构造映射表 S_s，将 16 位随机数字纵向映射成 16 字节密钥 K_a = AC7kzPxyTo1PTJlC，用 K_a 对明文加密得到密文文件 Cipher。同时，用 Pub_s 加密 K_a 得到 K_a'封装在文件中。最后，由客户端将密文文件和 K_a'封装文件发送到服务器并存储。

4.1.2　审计端下载数据加密实验

主机模拟审计端发送请求，同时记录当前时间戳，产生随机数种子 Z_c，得到 $M_c=rand(Z_c X)$，其中 X 为审计人员编号 52150332112。M_c 对 62 进行取模运算得到表 3 所列的 20 位随机数字。

表 3　审计端产生的随机数字

52	59	53	32	61	51	43	36	2	60
40	32	6	14	37	60	47	19	30	15

审计端构建映射表 S_c，其是由 62 位包含大小写字母及数字组成的随机排列字母表，如表 4 所列。

表 4　S_c 映射表

5	g	x	G	O	o	Z	N	q	h	4	X	S	2	J	t
k	Q	R	q	Y	2	h	w	A	w	I	X	O	T	B	a
6	Q	F	9	e	J	t	3	a	R	G	w	u	o	I	Q
i	U	c	G	F	1	Q	P	d	B	p	5	s	C		

将表 3 产生的随机数在 S_c 映射表中进行纵向映射，得到私钥 Pri_c=si2PauGdktBPQqhtwew9。由私钥 Pri_c 计算可得公钥 Pub_c，封装在文件中传送给服务器。

服务器端接收到公钥 Pub_c 文件后用它加密 Pri_s 生成 Pri_s'封装成文件和 Cipher 文件及 K_a'一起发送给审计端。

审计端通过私钥 Pri_c = si2PauGdktBPQqhtwew9 解密 Pri_s'得到 Pri_s=ZTZrYxxgf1bW6cmcpqPT，再用 Pri_s 解密 K_a'，得到 K_a = AC7kzPxyTo1PTJlC。最后，用 K_a 解密 Cipher 得到明文。

4.2　HBES 优势分析

采用混合双向加密方案使数据在双向传输及存储过程中具有如下优势：

1）使用 AES 加密数据，ECC 加密密钥具有加密效率高、适用范围广等特点。

2）数据接收方产生的私钥由随机数通过映射规则得到，增强了密钥的安全性和不可伪造性，为数据的加密提供了本质安全保障。

3）在双向传输过程中，私钥由数据接收方产生并进行本地化存储，使得在网络中传输的只有公钥和密文。当密文在传输过程中被非法窃取，由于私钥的本地化存储，使得密文无法被解密从而保证明文的安全性。

4）云端存储数据以密文形式存储，增强了原始数据的安全性。由于云端采取的是分布式存储文件系统，提高了存储效率，同时具备了负载均衡和故障冗余功能。

5　性能分析

针对本文提出的 HBES，在保证该方案可行性的前提下，

（下转第 371 页）

ACM，2000，43(4)：99-105.
[5] LAU S. The spinning cube of potential doom[J]. Communications of the ACM，2004，47(6)：25-26.
[6] YURCIK B. Security Incident Fusion Tool (SIFT) Research Project[OL]. http://www.projects.ncassr.org/sift.
[7] 陈秀真，郑庆华，管晓宏，等. 网络化系统安全态势评估的研究[J]. 西安交通大学学报，2004，38(4)：404-408.
[8] 胡华平，张怡，陈海涛，等. 面向大规模网络的入侵检测与预警系统研究[J]. 国防科技大学学报，2003，25(1)：21-25.
[9] 任伟，蒋兴浩，锬锋. 基于 RBF 神经网络的网络安全态势预测方法[J]. 计算机工程与应用，2006，42(31)：136-138.
[10] 胡明明，王慧强，赖积保. 一种基于 GA-BPNN 的网络安全态势预测方法[EB/OL]. [2007-07-24]. http://www.paper.edu.cn/releasepaper/content/20070-437.
[11] 王宇飞，沈红岩. 基于改进广义回归神经网络的网络安全态势预测[J]. 华北电力大学学报，2011，38(3)：91-95.
[12] 丁硕，常晓恒，巫庆辉，等. GRNN 与 BPNN 的函数逼近性能对比研究[J]. 现代电子技术，2014，37(7)：114-117.
[13] 涂娟娟. 粒子群优化算法的几种改进算法及应用[D]. 南京：中国矿业大学，2014.
[14] 曹蓉蓉. 大数据环境下网络安全态势感知研究[J]. 数字图书馆论坛，2014(2)：85-91.
[15] 孟建良，刘德超. 一种基于 Spark 和聚类分析的辨识电力系统不良数据新方法[J]. 电力系统保护与控制，2016，44(3)：85-91.
[16] 胡俊，胡贤德，程家兴，等. 基于 Spark 的大数据混合计算模型[J]. 计算机系统应用，2015，24(4)：214-218.
[17] ZAHARIA M，DAS T，LI H，et al. Discretized streams：an efficient and fault-tolerant model for stream processing on large clusters[C]// Proceedings of the 4th USENIX conference on Hot Topics in Cloud Ccomputing. USENIX Association，2012.
[18] 涂娟娟. PSO 优化神经网络算法的研究及其应用[D]. 南京：江苏大学，2013.
[19] 唐振坤. 基于 Spark 的机器学习平台设计与实现[D]. 厦门：厦门大学，2014.
[20] 刘世成，张建华，刘宗岐，等. 并行自适应粒子群算法在电力系统无功优化中的应用[J]. 电网技术，2012，36(1)：108-112.

(上接第 335 页)

从安全和时间方面对其性能进行分析。

5.1　安全性能分析

本文所提出的 HBES 的安全性着重体现在 ECC 对私钥加密方面。由于 ECC 属于非对称加密算法，安全性优于对称加密算法，与其他对称加密算法相比，ECC 的安全性依赖于椭圆曲线上的离散对数问题(ECDLP)的求解困难性。研究表明迄今为止没有发现有效计算 ECDLP 的方法[6]。

可以看出 HBES 具有良好的安全性，因此可较好地适用于云审计中企业数据的加密。

5.2　时间性能分析

云审计数据侧重于对数据的加密上传过程，因此，基于加密耗时来衡量 HBES 的性能。通过比较 ECC 与 HBES 的加密耗时，验证该方法在保证安全性的前提下具有较快的加密速率。

以行为单位读取纯文本文件的方法对字符串进行加密，并把加密内容存储在另一个文件中，计算文件加密时间。加密大文件时，需在虚拟机中运行 32 位 Linux 系统，配置(－Xmx1535M－Xms1536M)设置内存大小。

图 5 反映了两种加密方式对应不同数据量时所花费时间的关系。对比图中数据可知，HBES 的加密时间远远小于 ECC 的加密时间。另外，对于较大数据，ECC 加密时间显著增加，而 HBES 呈平稳式上升。因此，该方法具有较好的加密效率，适用于云审计中大数据量的加密。

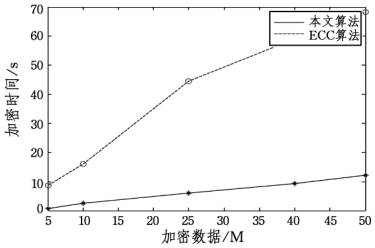

图 5　加密时间对比

结束语　本文对审计数据在网络中传输所带来的安全问题的基础上，引进了混合双向加密方案(HBES)，以保证待审计数据的安全性。HBES 引入了双向加密的概念，较之前的单向加密方法更加突出了从云端下载数据时的加密。提出在上传或下载数据时，由事件发起者产生 ECC 私钥，在网络传输过程中只有公钥和密文可见，而私钥则由发起者保存在本地系统中。当密文在传输过程中被非法窃取，由于私钥的本地化存储，使得密文无法被解密从而保证明文的安全性。通过相关模拟实验验证了 HBES 的可行性。由于实验所选取的是部分待审计数据，相对于真实云审计数据有一定差度，因此加密时间具有一定波动性。本文的方法旨在在使用 HBES 提高加解密速率的同时保证数据在传输过程中的安全性。

参 考 文 献

[1] 徐贵丽. 云审计：机遇、挑战与发展趋势[J]. 中国注册会计师，2014(3)：109-112.
[2] 陈恺. 2016 年 RSA 大会信息安全热点[J]. 信息技术与标准化，2016(3)：15-16.
[3] 秦荣生. 云计算的发展及其对会计、审计的挑战[J]. 当代财经，2013(1)：111-117.
[4] 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.
[5] KAUFMAN L M. Data security in the world of cloud computing[J]. IEEE Security & Privacy，2009，7(4)：61-64.
[6] REN K，WANG C，WANG Q. Security challenges for the public cloud[J]. IEEE Internet Computing，2012，16(1)：69-73.
[7] TRAPPE W，WASHINGTON L C. Introduction to cryptography with coding theory[M]. Pearson Education India，2006.
[8] 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.
[9] TEBAA M，EL HAJJI S，EL GHAZI A. Homomorphic encryption applied to the cloud computing security[C]// Proceedings of the World Congress on Engineering. 2012：4-6.
[10] 宗平，周明. 云计算中的数据安全存储和加密模型的设计[J]. 计算机技术与发展，2013(11)：137-140.
[11] 俞经善，王晶，杨川龙. 基于 ECC 和 AES 相结合的加密系统的实现[J]. 信息技术，2006，30(2)：44-46.
[12] 陈原. 公钥加密与混合加密的可证明安全性研究[D]. 西安：西安电子科技大学，2006.