一个改进的云存储数据完整性验证方案

周恩光[1,2],李舟军[1,2],郭 华[1,3],贾仰理[4]
(1.北京航空航天大学软件开发环境国家重点实验室,北京 100191;2.北京航空航天大学网络技术北京市重点实验室,北京 100191;
3.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093;4.聊城大学计算机学院,山东聊城 252059)

摘 要: 在云计算环境中,客户将数据存储在不可信的云存储服务器上.如何在本地没有数据副本的情况下,高效地对客户存储的远程数据进行完整性验证是一个亟待解决的问题,针对此问题已相继提出一系列解决方案.提出已知证据伪造攻击的概念,即拥有一定数量证据的敌手可以伪造新的合法证据.指出已有的一些数据完整性验证方案无法抵抗已知证据伪造攻击.利用基于等级的认证跳表提出一个改进方案,该方案支持完全数据更新和公开审计.

关键词: 云存储; 完整性验证; 公开审计; 数据更新
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2014)01-0150-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.01.024

An Improved Data Integrity Verification Scheme in Cloud Storage System

ZHOU En-guang[1,2], LI Zhou-jun[1,2], GUO Hua[1,3], JIA Yang-li[4]
(1. *State Key Laboratory of Software Development Environment*, *Beihang University*, *Beijing* 100191, *China*;
2. *Key Laboratory of Beijing Network Technology*, *Beihang University*, *Beijing* 100191, *China*;
3. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*;
4. *School of Computer*, *Liaocheng University*, *Liaocheng*, *Shandong* 252059, *China*)

Abstract: In cloud computing, clients put the large data files on the untrusted cloud storage server. As clients no longer physically possess the storage of their data, how to efficiently verify the correctness of outsourced cloud data becomes a big challenge for data storage security in cloud computing. In order to solve the problem of data integrity checking, many schemes are proposed. We first propose the notion of the known-proofs forgery attack, i.e., the adversary who has a certain number of proofs can forge a new legal proof. We point out that some known schemes cannot resist the known-proofs forgery attack. After that we propose an improved data integrity checking protocol with full data dynamics and public verifiability for cloud storage by manipulating rank-based authenticated skip list.

Key words: cloud storage; integrity authentication; public auditability; data dynamics

1 引言

在云计算环境中,客户将数据存储在不可信的云存储服务器(以下简称云服务器)上.因此,如何在本地没有数据副本的情况下,高效地对客户存储的数据进行完整性验证,是一个亟待解决的问题[1].针对此问题,目前已有一系列的解决方案[2~14].Ateniese 等人[2]利用同态标签首次提出支持公开审计的可证明数据持有方案(Provable Data Possession, PDP).随后,他们改进了该方案[8]以支持数据更新操作.文献[9]提出一个能定位错误数据的 PDP 方案.Juels 和 Kaliski 提出可恢复证明(Proof Of Retrievability, POR)方案[3],该方案可保证数据的完整性和可恢复性.Shacham 和 Waters 利用 BLS(作者 Boneh D, Lynn B 和 Shacham H 名字的缩写)签名[15]提出一个支持公开审计的 POR 方案[4],但该方案可泄露客户隐私信息.Wang 等人[12]利用随机掩码技术提出一个改进的方案,保护了客户的隐私信息.Bowers 等人提出设计 POR 方案的理论框架[5].文献[4,8,9,12]仅支持部分数据更新,不支持数据块的插入.Erway 等人提出基于等级的认证跳表(Rank-based Authenticated Skip List, RASL)的概念,利用 RASL 提出支持完全数据更新的 PDP 方案[10].Hao 等人提出一个支持隐私保护和完全数据更新的完整性验证方案[13].文献[14]提出一个支持完全数据更新的的验证方案.

收稿日期:2012-11-12;修回日期:2013-08-20;责任编辑:李勇锋
基金项目:国家自然科学基金(No.60973105, No.61170189, No.61300172, No.61370126);博士点基金(No.20111102130003, No.20121102120017);软件开发环境国家重点实验室自主课题(No.SKLSDE-2013ZX-19, No.SKLSDE-2012ZX-11);中央高校基本科研业务费专项资金(No.YWF-13-A02-13)

本文提出已知证据伪造攻击的概念,即对于特定的一组数据块,若敌手拥有一定数量的完整性证据,则可通过已知证据伪造新的合法证据.并指出方案[4,10,11,12,14]存在已知证据伪造攻击.本文利用 RASL 提出一个改进方案,该方案支持完全数据更新、公开审计和隐私保护,且能抵抗已知证据伪造攻击.

2 预备知识

2.1 双线性映射

G_1, G_2 和 G_T 是阶为素数 p 的循环群. g_1, g_2 分别是 G_1, G_2 的生成元.双线性映射 $e: G_1 \times G_2 \to G_T$ 具有如下性质:(1)可计算性,存在有效的算法能够计算 e;(2)双线性,对 $u \in G_1, v \in G_2$ 和 $a, b \in Z_p$ 有 $e(u^a, v^b) = e(u, v)^{ab}$;(3)非退化性,$e(g_1, g_2) \neq 1$.

2.2 基于等级的认证跳表

Erway 等人提出 RASL 的概念.图 1 是 RASL 的一个例子.

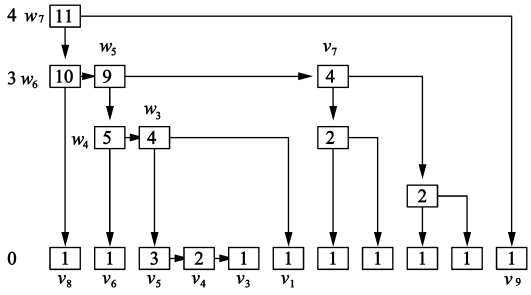

图1 基于等级的认证跳表

文件 $F = (m_1, m_2, \cdots, m_n)$.在 RASL 中,最左上的节点称为起始结点(即 w_7),每个节点 v 有两个指针 $rgt(v)$和 $dwn(v)$,分别指向节点 v 的右节点和下节点.在 RASL 中,节点 v 的等级(rank)定义为从节点 v 出发所能到达的底层节点的数量,用 $r(v)$表示.在图 1 中标注了每一个节点的等级.节点 v 的层数用 $l(v)$表示,$l(v)=0$表示节点 v 是底层节点.在 RASL 中,第 i 个底层节点 v 与数据块 m_i 对应,即节点 v 存储 $x(v) = m_i$.令多变量抗碰撞哈希函数 $h(x_1, x_2, \cdots, x_n) = h(h(x_1) \| h(x_2) \| \cdots \| h(x_n))$,"‖"为连接符.在 RASL 中,节点 v 的哈希值 $f(v)$为:

$$f(v) = \begin{cases} 0 & \text{if v = null} \\ h(l(v), r(v), x(v), f(rgt(v))) & \text{if } l(v) = 0 \\ h(l(v), r(v), f(dwn(v)), f(rgt(v))) & \text{if } l(v) > 0 \end{cases}$$

在 RASL 中,验证者要验证第 i 个数据块 m_i,证明者生成数据块 m_i 的证明信息 $\prod_i$.验证者利用证明信息 $\prod_i$ 能够对 m_i 的值和 m_i 的索引值 i 进行验证,在验证时验证者仅需要 RASL 起始节点的值.因篇幅限制,详细算法见文献[10].

3 已知证据伪造攻击及其应用场景

本节描述已知证据伪造攻击,即对于特定的一组数据块,若敌手拥有一定数量的完整性证据,则敌手可根据已知的证据伪造出新的合法证据.为方便描述攻击,本节规定如下:客户对文件 $F = (m_1, m_2, \cdots, m_n)$的 n 个数据块进行验证.

3.1 对 Wang 等人方案的攻击

Wang 等人的方案[12]的具体过程如下:

文件 $F = (m_1, m_2, \cdots, m_n)$, G_1, G_2 是阶为素数 p 的乘法群. e 为双线性映射, u 和 g 分别为 G_1 和 G_2 的生成元.哈希函数 $H(\cdot): \{0,1\}^* \to G_1$, $h(\cdot): G_1 \to Z_p$.客户私钥为 $sk = x$,其中 $x \in Z_p$,公钥为 $pk = (u, g, w, v)$,其中 $w = u^x$, $v = g^x$.客户计算数据块 m_i 的签名 $\sigma_i = (H(i) \cdot u^{m_i})^x$,将文件 F 和签名集合 $\{\sigma_i\}_{1 \le i \le n}$发送至云服务器.客户对文件 F 的 n 个数据块进行挑战.客户选择随机值 $\nu_i \in Z_p$, $1 \le i \le n$,发送挑战消息 $chal = \{(i, v_i)\}_{1 \le i \le n}$.云服务器生成随机数 $r \in Z_p$,计算 $R = w^r = (u^x)^r$, $\mu = \sum_{i=1}^{n} v_i m_i + rh(R)$和 $\eta = \prod_{i=1}^{n} \sigma_i^{v_i}$,将证据 $P = (\mu, \eta, R)$发送至客户.客户验证等式 $e(\eta \cdot (R^{h(R)}), g) = e(\prod_{i=1}^{n} H(i)^{v_i} \cdot u^{\mu}, v)$.

攻击:在 Wang 等人的方案中,若敌手通过窃听获得 n 个证据,则敌手在没有文件 F 的前提下,能够伪造文件 F 的新的合法证据.

其攻击过程如下:客户和云服务器之间成功地进行了 n 次完整性验证.敌手窃听并保存下面消息:

$$\{chal_1 = \{(i, v_{1i})\}, 1 \le i \le n, P_1 = (\mu_1, \eta_1, R_1)\},$$
$$\{chal_2 = \{(i, v_{2i})\}, 1 \le i \le n, P_2 = (\mu_2, \eta_2, R_2)\},$$
$$\cdots\cdots$$
$$\{chal_n = \{(i, v_{ni})\}, 1 \le i \le n, P_n = (\mu_n, \eta_n, R_n)\}.$$

其中 $P_i = (\mu_i, \eta_i, R_i)(1 \le i \le n)$是第 i 次完整性验证过程中,云服务器发送的证据.

敌手窃听获得 n 个证据 $P_i = (\mu_i, \eta_i, R_i), (1 \le i \le n)$,由 $\mu_j = \sum_{i=1}^{n} v_{ji} m_i + r_j h(R_j), (1 \le j \le n)$可得下面方程组:

$$\begin{cases} v_{11} m_1 + v_{12} m_2 + \cdots + v_{1n} m_n + r_1 h(R_1) = \mu_1 \\ v_{21} m_1 + v_{22} m_2 + \cdots + v_{2n} m_n + r_2 h(R_2) = \mu_2 \\ \vdots \\ v_{n1} m_1 + v_{n2} m_2 + \cdots + v_{nn} m_n + r_n h(R_n) = \mu_n \end{cases}$$

令矩阵 $\boldsymbol{V} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{bmatrix}$,

令向量 $\boldsymbol{V}_1=(v_{11},v_{12},\cdots,v_{1n})$,

$\boldsymbol{V}_2=(v_{21},v_{22},\cdots,v_{2n})$,$\cdots$,

$\boldsymbol{V}_n=(v_{n1},v_{n2},\cdots,v_{nn})$.

令 $\det(\boldsymbol{V})\neq 0$,则向量 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_n$ 线性无关.此时,敌手收到新的挑战消息 $chal^*=\{(1,v_1^*),(2,v_2^*),\cdots,(n,v_n^*)\}$,

令 $\boldsymbol{V}^*=(v_1^*,v_2^*,\cdots,v_n^*)$,根据矩阵理论可知,存在不全为 0 的整数 $\lambda_1,\lambda_2,\cdots,\lambda_n$,使得 $\boldsymbol{V}^*=\lambda_1\boldsymbol{V}_1+\lambda_2\boldsymbol{V}_2+\cdots+\lambda_n\boldsymbol{V}_n$.

令 $\mu'=\lambda_1\mu_1+\lambda_2\mu_2+\cdots+\lambda_n\mu_n$, $\eta^*=\prod_{i=1}^{n}(\eta_i\cdot R_i^{h(R_i)})^{\lambda_i}$.

敌手生成随机数 $r^*\in Z_p$,计算 $R^*=w^{r^*}=(u^x)^{r^*}$ 和 $\mu^*=\mu'+r^*h(R^*)$.因为:

$$e(\eta^*,g)=e(\prod_{i=1}^{n}(\eta_i\cdot R_i^{h(R_i)})^{\lambda_i},g)$$

$$=\prod_{j=1}^{n}e(\prod_{k=1}^{n}H(k)^{v_{jk}}\cdot u^{\mu_j},v)^{\lambda_j}$$

$$=\prod_{j=1}^{n}e(\prod_{k=1}^{n}H(k)^{v_{jk}\cdot\lambda_j}\cdot u^{\lambda_j\cdot\mu_j},v)$$

$$=e(\prod_{k=1}^{n}H(k)^{v_k^*}\cdot u^{\mu'},v),$$

$$e(\eta^*\cdot(R^{*h(R^*)}),g)=e(\prod_{i=1}^{n}H(i)^{v_i^*}\cdot u^{\mu'+r^*h(R^*)},v)$$

$$=e(\prod_{i=1}^{n}H(i)^{v_i^*}\cdot u^{\mu^*},v),$$

所以证据 $P^*=(\mu^*,\eta^*,R^*)$可通过验证,敌手在没有文件 F 的前提下成功伪造一个合法的证据.在伪造过程中,客户在云服务器上存储的 n 个数据均未泄露,即敌手未获得客户的任何数据.

同理,文献[4,10,14]也存在类似的攻击.在文献[11]中,验证者在挑战时产生两个随机数,若重用第一个随机数,则也会导致已知证据伪造攻击.

3.2 已知证据伪造攻击的应用场景

敌手在下面两场景中可利用已知证据伪造攻击对客户进行欺骗.

(1)敌手假冒云服务器,对客户进行欺骗.

敌手拥有 n 个完整性证据.客户发起新的挑战 $chal^*=\{(i,v_i^*)\}$,$1\le i\le n$,敌手将客户的挑战信息 $chal^*$ 截获,然后利用已知证据伪造攻击伪造一个新的合法证据.客户认为,只有云服务器才能产生合法的证据,因此敌手成功地假冒了云服务器.

(2)云服务器在客户数据丢失的情况下,利用已知证据伪造攻击对客户进行欺骗.

首先,客户和云服务器成功地进行了 n 次完整性验证(云服务器拥有 n 个完整性证据).随后,云服务器发生故障导致客户的数据被删除.此时,客户发起新的完整性挑战.云服务器为了隐瞒客户数据丢失的真相,利用已知证据伪造攻击,伪造一个新的合法证据 P^*,使客户仍然相信存储数据的完整性.

4 改进方案

4.1 方案定义

改进方案包括 4 个算法,定义如下:

$(pk,sk)\leftarrow KeyGen(1^k)$:输入安全参数 k,输出客户的公私钥对(pk,sk);

$(\Phi)\leftarrow SigGen(sk,F)$:输入私钥 sk 和文件 F,输出数据块签名集合 Φ.客户计算 RASL 起始节点的哈希值 M_s;

$(P)\leftarrow GenProof(F,chal,\Phi)$:输入文件 F,签名集合 Φ 和挑战消息 $chal$,输出 $chal$ 中指定数据块的完整性证据 P;

$(TRUE,FALSE)\leftarrow VerifyProof(pk,chal,P)$:输入公钥 pk,证据 P 和挑战消息 $chal$,如果验证通过输出 $TRUE$,否则输出 $FALSE$.

4.2 方案的具体过程

$KeyGen(1^k)$:G_1,G_2 是阶为素数 p 的乘法群.e 为双线性映射,u 和 g 分为 G_1 和 G_2 的生成元.哈希函数 $h(\cdot):G_1\rightarrow Z_p$.客户私钥为 $sk=x$,其中 $x\in Z_p$,公钥为 $pk=(u,g,w,v)$,其中 $w=u^x$,$v=g^x$.

$SigGen(sk,F)$:客户为数据块 m_i 生成签名 $\sigma_i=(u^{m_i})^x$.RASL 的底层节点为按照顺序排列的签名 $\sigma_i=(u^{m_i})^x$,$(1\le i\le n)$,即 $x(v_i)=\sigma_i$.客户计算 RASL 的起始节点哈希值 M_s(M_s 为公开变量).客户将$\{F,\{\sigma_i\}_{1\le i\le n}\}$和 RASL 发送至云服务器后,删除$\{F,\{\sigma_i\}_{1\le i\le n}\}$和 RASL.

客户从集合$\{1,2,\cdots,n\}$中随机选择 c 个元素组成集合 $I=\{s_1,s_2,\cdots,s_c\}$,其中 $s_1<\cdots<s_c$.对 $i\in I$,客户选择随机值 $\nu_i\in Z_p$.客户将挑战消息 $chal=\{(i,v_i)\}_{s_1\le i\le s_c}$发送至云服务器.

$GenProof(F,chal,\Phi)$:云服务器先生成挑战数据块的签名 $\{\sigma_i\}_{s_1<i<s_c}$ 在 RASL 中的证明信息 $\{\prod_i\}_{s_1<i<s_c}$,然后生成随机数 $r\in Z_p$,计算 $R=w^r=(u^x)^r$,令 $\mu'=\sum_{i=s_1}^{s_c}v_im_i$,计算 $\mu=\mu'+rh(R)$.云服务器发送证据 $P=\{\mu,R,\{\sigma_i,\prod_i\}_{s_1<i<s_c}\}$.

$VerifyProof(pk,chal,P)$:客户收到证据 P 后,首先对$\{\sigma_i,\prod_i\}_{s_1<i<s_c}$进行验证(可对 σ_i 的值和σ_i 的索引值 i 进行验证).如果验证成功,客户计算 $\eta=\prod_{i=s_1}^{s_c}\sigma_i^{v_i}$,验证

等式 $e(\eta\cdot(R^{h(R)}),g)=e(u^{\mu},v)$. 如果验证成功,客户输出 TRUE,否则客户输出 FALSE.

在改进方案中,利用 RASL 对消息 $\{\sigma_i\}_{s_1<i<s_c}$ 进行认证,故客户计算 $\eta=\prod_{i=s_1}^{s_c}\sigma_i^{v_i}$ 的值是唯一确定的,进而可以抵抗已知证据伪造攻击.

改进方案具有以下性质:

完全数据更新:利用 RASL 使改进方案支持数据块的插入、删除和修改;

公开审计:任何人,不仅是数据的拥有者,都能对客户存储的数据进行完整性验证. 在改进方案中,验证者只需客户公钥和 RASL 起始节点的哈希值 M_s 等公开信息就可以进行完整性验证;

隐私保护:在验证过程中,不泄露客户存储数据的隐私信息.

5　安全性及性能分析

定理 1　若云服务器通过完整性验证,则存在一个提取器能够恢复客户挑战的数据块.

证明与文献[12]类似. 将云服务器视为敌手,提取器控制随机预言机 $h(\cdot)$ 回答云服务器的哈希询问. 对于询问 R,提取器输出 $\theta=h(R)$,然后云服务器输出证据 $P=(\mu,R,\{\sigma_i,\prod_i\}_{s_1<i<s_c})$. 提取器重绕(rewind)至输出 $\theta=h(R)$ 的前一刻,提取器输出 $\theta^*=h(R)$ 并且 $\theta\neq\theta^*$,云服务器输出 $P=(\mu^*,R,\{\sigma_i,\prod_i\}_{s_1<i<s_c})$. 综上得 $\mu^*=\sum_{i=s_1}^{s_c}v_im_i+r\theta^*=\mu'+r\theta^*$,$\mu=\sum_{i=s_1}^{s_c}v_im_i+r\theta=\mu'+r\theta$,则提取器可得 $\{\eta,\mu'=\sum_{i=s_1}^{s_c}v_im_i=(\theta\mu^*-\theta^*\mu)/(\theta-\theta^*)\}$. 根据文献[4]中的定理 4.2 可知,提取器可以恢复挑战的数据块.

令 E 表示群 G 中一次指数计算的时间,即计算 g^x 的所需要时间,其中 x 为 Z_p 中的整数,$g\in G$. 令 B 表示一次双线性映射 $e(\cdot,\cdot)$ 的计算时间. Z_p 中的代数运算以及哈希运算所需要的时间可以忽略不计. 在改进方案中,验证者的计算代价为 $(c+2)|E|+2|B|$,云服务器的计算代价为 $|E|$,其中 c 为验证者挑战的数据块的个数.

6　结论

本文提出已知证据伪造攻击的概念,并指出已有的一些数据完整性验证方案不能抵抗已知证据伪造攻击. 同时利用 RASL 提出了一个能够抵抗已知证据伪造攻击的改进方案. 该方案支持完全数据更新和公开审计,并且能够保护客户数据的隐私.

参考文献

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

[2] G Ateniese, R Burns, R Curtmola, J Herring, L Kissner, Z Peterson, D Song. Provable data possession at untrusted stores [A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. Alexandria: ACM, 2007. 598 – 609.

[3] Juels, Burton S Kaliski Jr. Pors: Proofs of retrievability for large files[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security [C]. Alexandria: ACM, 2007. 584 – 597.

[4] H Shacham, B Waters. Compact proofs of retrievability[A]. Proceedings of the 14th International Conference on Theory and Application of Cryptology and Information Security: Advances in Cryptology[C]. Melbourne: LNCS 5350, 2008. 90 – 107.

[5] K D Bowers, A Juels, A Oprea. Proofs of retrievability: Theory and implementation[A]. Proceedings of the 2009 ACM Workshop on Cloud Computing Security[C]. Chicago: ACM, 2009. 43 – 54.

[6] Ee-Chien Chang, Jia Xu. Remote integrity check with dishonest storage server[A]. Proceedings of the 13th European Symposium on Research in Computer Security[C]. Berlin: Springer-Verlag, 2008. 223 – 237.

[7] A Oprea, MK Reiter, K Yang. Space – efficient block storage integrity[A]. Proceedings of the 12th Annual Network and Distributed System Security Symposium[C]. San Diego: USENIX, 2005. 1 – 12.

[8] G Ateniese, RD Pietro, LV Mancini, G Tsudik. Scalable and efficient provable data possession [A]. Proceedings of the 4th International Conference on Security and Privacy in Communication Networks[C]. Istanbul: ACM, 2008. 1 – 10.

[9] C Wang, Q Wang, K Ren, W Lou. Ensuring data storage security in cloud computing[A]. Proceedings of the 17th International Workshop Quality of Service [C]. Charleston: IEEE, 2009. 1 – 9.

[10] C Erway, A Kupcu, C Papamanthou, R Tamassia. Dynamic provable data possession[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security[C]. Chicago: ACM, 2009. 213 – 222.

[11] F Sebe, J Domingo-Ferrer, A Martinez-Balleste, Y Deswarte, J-J Quisquater. Efficient remote data possession checking in critical information infrastructures[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8): 1034 – 1038.

[12] C Wang, Q Wang, K Ren, W Lou. Privacy-preserving public

auditing for data storage security in cloud computing[A]. Proceedings of 2010 IEEE INFOCOM[C]. San Diego: IEEE, 2010.1 – 9.

[13] Zhuo Hao, Sheng Zhong, Nenghai Yu. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability[J]. IEEE Transactions on Knowledge and Data Engineering, 2011, 23(9): 1432 – 1437.

[14] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li. Enabling public auditability and data dynamics for storage security in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847 – 859.

[15] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297 – 319.

作者简介

周恩光 男. 1984 年 3 月生, 河北鹿泉人. 北京航空航天大学计算机学院博士研究生. 研究方向为信息安全、云计算安全.

E-mail: enguangzhou@163.com

李舟军 男. 1963 年 9 月生, 湖南湘乡人. 1999 年获国防科技大学计算机博士学位. 现为北京航空航天大学计算机学院信息安全系主任、教授、博士生导师. 主要研究兴趣为网络与信息安全、数据挖掘与社交网络分析.

E-mail: lizj@buaa.edu.cn