·安全技术· 文章编号：1000-3428(2014)11-0118-03 文献标识码：A 中图分类号：TP309

一种可验证的公钥可搜索加密方案

刘鹏亮，俎龙辉，白翠翠，马 华

（西安电子科技大学数学与统计学院，西安 710071）

摘 要： 公钥可搜索加密能实现基于密文的信息检索，适用于云计算环境。但现有公钥可搜索加密方案普遍依赖于双线性对，并且无法对服务器返回的搜索结果进行验证，效率和安全性较低。为此，基于 ElGamal 加密算法提出一种可验证的公钥可搜索加密方案。该方案使用 ElGamal 加密算法替代双线性对运算，与传统算法相比具有较低的计算复杂度，并且易于实现。在密文关键词及加密文件生成算法中，采用 ElGamal 签名算法对关键词的哈希值进行数字签名。当收到服务器返回的搜索结果后，用户可以通过计算得到发送者的公钥，并对相应的签名值进行验证，从而有效防止服务器返回错误结果。

关键词： 可搜索加密；公钥；密文关键词；验证；关键词搜索；ElGamal 加密

中文引用格式： 刘鹏亮，俎龙辉，白翠翠，等. 一种可验证的公钥可搜索加密方案[J]. 计算机工程，2014，40(11)：118-120.

英文引用格式： Liu Pengliang，Zu Longhui，Bai Cuicui，et al. A Verifiable Public Key Searchable Encryption Scheme[J]. Computer Engineering，2014，40(11)：118-120.

A Verifiable Public Key Searchable Encryption Scheme

LIU Pengliang，ZU Longhui，BAI Cuicui，MA Hua

（School of Mathematics and Statistics，Xidian University，Xi'an 710071，China）

【Abstract】 As an attractive cryptographic primitive，the public key searchable encryption enables users to search on encrypted data，and hence is applicable to the setting of cloud computing. But most of the existing schemes have to adopt the bilinear pairing and fail to verify search results from the server. Accordingly，these schemes suffer drawbacks in terms of efficiency and security. Aiming at this problem，based on the ElGamal encryption algorithm，a new verifiable scheme is proposed. It has more desirable computation efficiency and is easy to implement in because it replaces the bilinear pairing with the ElGamal encryption. Especially，during the generation of encrypted keywords and encrypted files，the new scheme can generate the digital signature of the hash value of keywords based on the ElGamal signature algorithm. Upon receiving the search results from the server，users can obtain the public key of the sender，and then verify the ElGamal signature，which effectively prevents the server from returning wrong results.

【Key words】 searchable eneryption；public key；encrypted keyword；verification；keyword search；ElGamal encryption

DOI： 10.3969/j.issn.1000-3428.2014.11.023

1 概述

随着云计算技术越来越流行，大量的私密信息被存储在云端[1-2]。因此，云端数据的安全性引起了广泛关注。加密技术保护了数据的机密性和隐私性，却给加密数据的检索带来了很大的困难。检索加密数据的一种方法是用户将所有密文全部下载，逐一解密寻找自己想要的文件，确保了不会泄露任何信息给服务器。这是一项非常耗时且需要很大存储空间的任务，对资源受限的用户来说，寻找特定文件是不现实的。为使用户在不解密密文的情况下快速找到自己想要的文件，研究者提出了可搜索加密方法[3]，主要分为公钥可搜索加密[4-5]和对称可搜索加密[6-7]。目前许多公钥可搜索加密方案相继被提出，如文献[8-9]通过利用改变传统陷门信息解决了公钥可搜索加密中存在的陷门攻击问题，增强了方案的安全性。但其方案都是基于计算量大且难以实现的双线性对。针对这一缺陷，文献[10]基于 K-容

基金项目： 国家自然科学基金资助项目(61100229)；中央高校基本科研业务费专项基金资助项目(K5051270003)；信息安全国家重点实验室开放基金资助项目(GW0704127001)；陕西省教育厅科研计划基金资助项目(12JK0852)。

作者简介： 刘鹏亮(1988－)，男，硕士研究生，主研方向：网络与信息安全；俎龙辉、白翠翠，硕士研究生；马 华，教授。

收稿日期： 2013-12-23 **修回日期：** 2014-01-19 **E-mail：** ffgz112lpl@126.com

忍的身份加密技术提出了一种新的公钥可搜索加密方案,方案中运用多项式和异或运算代替双线性对,提高了计算效率。文献[11]提出了一种基于大整数分解的公钥可搜索加密方案。然而,上述方案都存在着一个共同的问题:均没有对搜索结果进行正确性验证。而与公钥相对应的对称可搜索加密中已经实现了对搜索结果的验证。文献[6-7]分别提出了对称可搜索加密中确定性和模糊性关键词搜索结果的验证方案,确保了用户对服务器返回结果的正确性和完整性的验证。

针对公钥可搜索加密中缺少验证这一问题,本文基于离散对数问题,运用 ELGamal 算法构造一种可验证的公钥可搜索加密方案。

2　预备知识

2.1　ELGamal 加密算法

ELGamal 加密算法不是一个确定性算法,其加密结果依赖于消息、公钥和一个随机选择的数,算法具体过程如下:

(1)密钥生成:Z_p 是有 p 个元素的有限域,p 是一个大素数,g 是 Z_p^* 中的一个生成元。选择随机整数 x,$0\leqslant x\leqslant p-2$,计算 $y=g^x \bmod p$,则公钥为(p,g,y),其中,p,g 可由一组用户共享,私钥为 x。

(2)加密:若加密明文消息为 M,发送者选择随机整数 $k(1\leqslant k\leqslant p-1)$,并且 $\gcd(k,p-1)=1$。计算 $y_1=g^k$,$y_2=My^k=Mg^{xk}$,则密文为 $C=\langle y_1,y_2\rangle$。

(3)解密:当接收者接收到密文 C 后,利用私钥 x 恢复 $M=\dfrac{y_2}{y_1^x}=\dfrac{Mg^{xk}}{(g^k)^x}$。

2.2　ELGamal 签名算法

ELGamal 签名算法的具体过程如下:

(1)密钥生成(同 ELGamal 加密算法):公钥为(p,g,y),私钥为 x。

(2)签名:对明文消息 M,进行如下操作:

选择随机整数 $k(1\leqslant k\leqslant p-2)$,这里 k 必须满足并且 $\gcd(k,p-1)=1$;$r=g^k \bmod p$,$s=k^{-1}(M-rx) \bmod (p-1)$,则签名消息为$(M,r,s)$。

(3)验证:当接收者收到签名消息(M,r,s)后进行如下计算:1)验证是否有 $1\leqslant r\leqslant p-1$,如果不是,则拒绝签名;2)计算 $v=g^M$ 和 $w=y^r r^s$;3)如果 $v=w$ 成立,则接受签名,否则拒绝。

3　方案构造

公钥可搜索加密方案模型如图 1 所示。发送者(Alice)利用接收者(Bob)的公钥生成密文关键词并将密文存储于服务器。Bob 用自己的私钥生成陷门发送给服务器,然后服务器检测密文关键词和陷门是否是由同一个关键词生成。如果相同,服务器就发送密文给接收者。否则,返回空值。

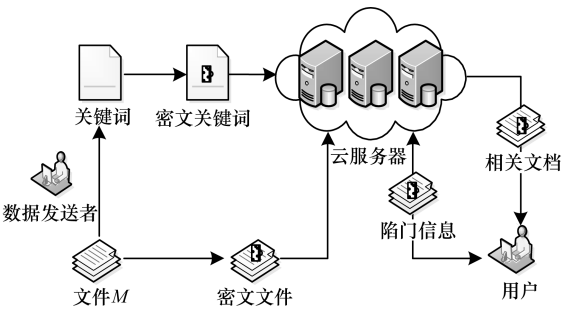

图 1　公钥可搜索加密模型

本文基于 ELGamal 加密和签名算法构造了一种新可验证的公钥可搜索加密方案。新方案不仅实现了关键词的检索,而且 Bob 可以对服务器返回的搜索结果的正确性进行验证。新方案包括 5 个算法:

(1)参数生成算法

首先 Alice 运行 ELGamal 加密算法,选择一个大素数 p_1,g_1 是 $Z_{p_1}^*$ 中的一个生成元。选择随机整数 $x_1(0\leqslant x_1\leqslant p-2)$,计算 $y_1=g_1^{x_1}$,Alice 公钥为(p_1,g_1,y_1),私钥为 x_1。选取 g_2 和 g 分别为 $Z_{p_2}^*$和 Z_p^* 的生成元,Bob 公钥为(p_2,g_2,y_2),私钥为 x_2;服务器公钥为(p,g,y),私钥为 x,哈希函数 $H:\{0,1\}^* \rightarrow Z_p^*$。

(2)密文关键词及加密文件生成算法

若 Alice 要发送含有关键词 w 的文件 M 给 Bob。Alice 计算关键词 W 的哈希值 $H(W)$,选取 2 个随机数 r_1,$r_2\in Z_p^*$,计算 $S_1=r_1 r_2^{H(w)} \bmod p$,$S_2=r_1^{H(w)^{-1}} r_2 \bmod p$,则密文关键词为 $S=\langle S_1,S_2\rangle$。

Alice 用 Bob 的公钥(p_2,g_2,y_2)对文件 M 进行加密:选择随机整数 $k(1\leqslant k\leqslant p_2-1)$,且$\gcd(k,p_2-1)=1$,计算 $y_{11}=g_2^k \bmod (p_2-1)$,$y_{12}=My_2^k \bmod (p_2-1)=Mg_2^{x_2 k} \bmod (p_2-1)$,密文为 $C_1=\langle y_{11},y_{12}\rangle$。

Alice 用自己的私钥 x_1 对 $H(w)$ 进行签名:选择随机整数 k_1,$k_1(1\leqslant k_1\leqslant p_1-1)$,$r=g_1^{k_1} \bmod (p_1-1)$,$s=k_1^{-1}(H(w)-rx_1) \bmod (p_1-1)$,则签名为 $sig=\langle H(w),r,s\rangle$。

为了让 Bob 确定此消息是来自 Alice,Alice 需对自己的身份 ID_A 用 Bob 的公钥(p_2,g_2,y_2)进行加密:选择随机整数 $k_2(1\leqslant k_2\leqslant p_2-1)$,计算 $y_{21}=g_2^{k_2} \bmod p_2$,$y_{22}=ID_A y_2^{k_2}=ID_A g_2^{x_2 k_2} \bmod p_2$,则身份密文为 $C_2=\langle y_{21},y_{22}\rangle$,最后 Alice 将密文关键词 $S=\langle S_1,S_2\rangle$和 $D=\langle C_1,sig,C_2\rangle$发送给服务器。

(3)陷门生成算法

当 Bob 要检索一个含有关键词 w_1 的文件时,他首先计算 $A=H(w_1)$,然后用服务器的公钥(p,g,y)对其进行加密。选择随机整数 $\alpha(1\leqslant\alpha\leqslant p-1)$。计

算 $y_{31}=g^{\alpha}\bmod p$;$y_{32}=Ag^{\alpha}\bmod p$;$T_W=Enc(A)=\langle y_{31},y_{32}\rangle$。Bob 将 T_w 发给服务器,作为对关键词 w 的搜索请求。

(4)检测算法

当服务器接收到来自 Bob 的搜索请求后,首先解密获取陷门信息。如果 $S_1=S_2^{H(w_1)}$,服务器返回 $D=\langle C_1,sig,C_2\rangle$ 发送给 Bob。否则,返回空值。

(5)验证算法

当 Bob 收到服务器返回的结果 D 后并将其分成 C_1,sig 和 $C_2$3 个部分,首先对身份密文 C_2 进行解密,确认发送者身份。然后再用其公钥对关键词的签名进行验证,若验证成功再对 C_1 进行解密。否则,丢弃。

方案正确性验证过程如下:

(1)Alice 计算:

$S=\langle S_1,S_2\rangle$,$D=\langle C_1,sig,C_2\rangle$

$S_1=r_1r_2^{H(w)}\bmod p$,$S_2=r_1^{H(w)^{-1}}r_2\bmod p$

$C_1=\langle y_{11},y_{12}\rangle=\langle g_2^k,Mg_2^{x_2k}\rangle$

$C_2=\langle y_{21},y_{22}\rangle=\langle g_2^{k_2},ID_Ag_2^{x_2k_2}\rangle$

$sig=(H(w),r,s)=$

$\langle H(w),g_1^k,k_1^{-1}(H(w)-rx_1)\bmod(p_1-1)\rangle$

Bob 计算:

$T_W=Enc(A)=\langle y_{31},y_{32}\rangle$

$y_{31}=g^{\alpha}\bmod p$,$y_{32}=Ag^{\alpha}\bmod p$

(2)服务器收到陷门信息,首先计算 $S_2^{H(w_1)}=(r_1^{H(w)^{-1}}r_2)^{H(w_1)}$,若 $w=w_1$,则有 $S_1=S_2^{H(w_1)}$。否则说明没有找到要查询的关键词。

(3)若 Bob 收到服务器返回的 $D=\langle C_1,sig,C_2\rangle$,首先进行身份验证:

1)对 C_2 进行解密计算,确认发送者的身份:

$$ID_A=\frac{y_{22}}{y_{21}^{x_1}}=\frac{ID_Ag_2^{x_1k_2}}{(g_2^{k_2})^{x_1}}$$

2)若上步身份验证是 Alice 时,用其公钥进行签名验证:

①验证是否有 $1\leqslant r\leqslant p_1-1$,如果不是,则拒绝该签名;

②计算 $v=g_1^{H(w_1)}$,$z=y_1^rr^s=(g_1^{x_1})^r\cdot(g_1^{k_1})^{k_1^{-1}(H(w)-rx_1)}=g_1^{H(w)}$,如果 $v=z$ 成立,则接受签名,否则拒绝。

3)解密:签名验证成功后 Bob 用自己的私钥对加密文件进行解密:

$$M=\frac{y_{12}}{y_{11}^{x_2}}=\frac{Mg_2^{x_2k}}{(g_2^k)^{x_2}}$$

通过以上分析,可以证明此方案是正确的。

4 安全性及效率分析

本文方案采用的是 ELGamal 加密和签名算法,接下来从 3 个方面对其安全性进行分析:

(1)文件密文和陷门信息安全性:对文件和陷门信息的加密都采用 ELGamal 加密算法,该算法基于求解离散对数困难问题。攻击者要通过求解离散对数得到解密密钥,而求解过程非常复杂。因此,保证了密文和陷门信息的安全性。

(2)签名安全性:对关键词 w,同样采用基于求解离散对数困难问题的 ELGamal 签名算法。每次选取不同的随机数 k_1 实施签名。这样即使同样的文件,得到的签名结果是不一样的,防止了重复攻击,提高了系统的安全性。另外,对密文关键词 w 的签名实质是对 $H(w)$ 的签名,所选取哈希函数是抗碰撞的,因此,对一个消息的签名伪造是不可能实现的。

(3)密文关键词安全性

关键词的密文形式 $S=\langle S_1,S_2\rangle$。其中:

$S_1=r_1r_2^{H(w)}\bmod p$,$S_2=r_1^{H(w)^{-1}}r_2\bmod p$

对每一个关键词 w 的加密都随机选取 r_1,r_2,攻击者无法直接获取有关关键词的任何信息。

文献[4,8-9]方案主要基于双线性对进行大量运算,这会耗费大量时间和存储资源。文献[10-11]基于大整数分解实现了公钥可搜索加密,提高了效率,却未对服务器的返回结果进行验证。本文基于 ELGamal 算法提出了一种新的可验证的公钥可搜索加密方案,利用 ELGamal 签名算法对搜索结果的正确性进行了验证。各种方案的比较如表 1 所示。

表 1 方案性能对比

方案	运算	有无验证
文献[4]方案	双线性对	无
文献[8]方案	双线性对	无
文献[9]方案	双线性对	无
文献[10]方案	多项式和异或	无
文献[11]方案	大整数分解	无
本文方案	离散对数	有

5 结束语

目前对公钥可搜索加密方案的研究较多,但多数方案中对服务器返回的搜索结果却未实现验证,而与之对应的对称可搜索加密已经实现了高效的验证。本文基于 ELGamal 算法构造了一种新的可验证的公钥可搜索加密方案,对服务器返回的结果的正确性进行了验证,并对方案从效率和安全性上进行了分析。下一步将研究如何对公钥可搜索加密中服务器返回的搜索结果进行更广泛的验证。

(下转第 125 页)

5　结束语

本文在分析时延容忍传感器网络模型的基础上,针对传感器网络中的黑洞攻击,提出一种利用传递证据和信任评价的恶意节点检测策略,并将其与路由协议进行融合。实验结果显示,本文提出的安全路由协议可以准确地检测出恶意节点并维持路由性能。采取多副本策略可以有效地抵御黑洞攻击,但多副本策略势必会增加节点的能耗,而传感器网络中节点的能量通常是有限的,因此,下一步需要研究如何在节点能耗允许的情况下,适当利用多余副本来抵御黑洞攻击。同时,还将研究传感器网络中其他攻击行为与防御策略。

参考文献

[1] Vasilescu I, Kotay K, Rus D. Data Collection, Storage, and Retrieval with an Underwater Sensor Network[C]//Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems. New York, USA: ACM Press, 2005: 154-165.

[2] Juang P, Oki H, Wang Yong, et al. Energy-efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet[J]. SIGARCH Computer Architecture News, 2002, 30(5): 96-107.

[3] Campbell A, Eisenman S, Lane N, et al. People Centric Urban Sensing [C]//Proceedings of WICON'06. Los Alamitos, USA: IEEE Computer Society, 2006: 2-5.

[4] 廖　俊,刘耀宗,姜海涛. 基于人工免疫的 MANET 不端行为检查模型[J]. 南京理工大学学报, 2011, 35(5): 652-658.

[5] Khalil I, Bagchi S, Rotaru C N, et al. UnMask: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks[J]. Ad Hoc Networks, 2010, 8(2): 148-164.

[6] 徐　佳,李千目,张　宏,等. 机会网络中的自适应喷雾路由及其性能评估[J]. 计算机研究与发展, 2010, 47(9): 1622-1632.

[7] Chuah M, Yang P, Han J. A Ferry-based Intrusion Detection Scheme for Sparsely Connected Ad Hoc Networks[C]//Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services. [S. l.]: IEEE Press, 2007: 1-8.

[8] Ren Yanzhi, Chuah M C, Yang J, et al. MUTON: Detecting Malicious Nodes in Disruption-tolerant Networks[C]//Proceedings of WCNC'10. [S. l.]: IEEE Press, 2010: 1-6.

[9] Dini G, Duca A L. Towards a Reputation-based Routing Protocol to Contrast Blackholes in a Delay Tolerant Network[J]. Ad Hoc Networks, 2012, 10(7): 1167-1178.

[10] Saha S, Verma R, Sengupta S, et al. SRSnF: A Strategy for Secured Routing in Spray and Focus Routing Protocol for DTN[C]//Proceedings of ACITY'12. Chennai, India: [s. n.], 2012: 159-169.

[11] Shah R C, Roy S, Jain S, et al. Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks[C]//Proceedings of the 1st International Workshop on Sensor Network Protocols and Applications. [S. l.]: IEEE Press, 2003: 30-41.

[12] Ren Yanzhi, Chuah M C, Yang Jie, et al. Detecting Blackhole Attacks in Disruption-tolerant Networks Through Packet Exchange Recording[C]//Proceedings of WoWMoM'10. [S. l.]: IEEE Press, 2010: 1-6.

[13] Ari K, Jörg O, Teemu K. The ONE Simulator for DTN Protocol Evaluation[C]//Proceedings of ACM International Conference on Simulation Tools and Techniques. New York, USA: ACM Press, 2009: 1-10.

编辑　金胡考

(上接第 120 页)

参考文献

[1] Wang Cong, Chow S S M, Wang Qian, et al. Privacy Preserving Public Auditing for Secure Cloud Storage[J]. IEEE Transactions on Computers, 2013, 62(2): 362-375.

[2] 聂规划,佘其平,陈冬林. 客户云需求波动下的多实例组合决策研究[J]. 计算机工程, 2013, 39(5): 43-47.

[3] Song X D, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]//Proceedings of 2000 IEEE Symposium on Security and Privacy. [S. l.]: IEEE Press, 2000: 44-55.

[4] Baek J, Safiavi-Naini R, Susilo W. Public Key Encryption with Keyword Search Revisited [C]//Proceedings of International Conference on Computational Science and Its Applications. Perugia, Italy: Springer-Verlag, 2008: 1249-1259.

[5] 方黎明. 带关键字搜索公钥加密的研究[D]. 南京: 南京航空航天大学, 2012.

[6] Chai Qi, Gong Guang. Verifiable Symmetric Searchable Enryption for Semi-honest But-curious Servers [EB/OL]. [2013-12-25]. http://www.cacr.math.Uwater-loo.ca/techreports/2011/cacr201122.

[7] Li Jin, Wang Qian, Wang Cong, et al. Fuzzy Keyword Search over Encrypted Data in Cloud Computing[C]//Proceedings of IEEE INFOCOM'10. [S. l.]: IEEE Press, 2010: 1-5.

[8] Rhee H S, Park J H, Susilo W, et al. Improved Searchable Public Key Encryption with Designated Tester [C]//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney, Australia: ACM Press, 2009: 376-379.

[9] Zhao Yuanjie, Chen Xiaofeng, Ma Hua, et al. A New Trapdoor-indistinguishable Public Key Encryption with Keyword Search[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2012, 3(1/2): 72-81.

[10] Yang Haomiao, Xu Chunxiang, Zhao Hongtian. An Efficient Public Key Encryption with Keyword Scheme Not Using Pairing[C]//Proceedings of the 1st International Conference on Instrumentation, Measurement, Computer, Communication and Control. Beijing, China: [s. n.], 2011: 900-904.

[11] Luo W, Tan J. Public Key Encryption with Keyword Search Based on Factoring [C]//Proceedings of CCIS'12. [S. l.]: IEEE Press, 2012: 1245-1247.

编辑　金胡考