·网络空间安全· 文章编号：1000-3428(2020)06-0136-08 文献标志码：A 中图分类号：TP393

电子邮件系统中支持关键字搜索的代理重加密方案

牛淑芬[a]，陈俐霞[a]，刘文科[a]，王彩芬[a]，杜小妮[b]

（西北师范大学 a. 计算机科学与工程学院；b. 数学与统计学院，兰州 730070）

摘 要： 针对在加密电子邮件系统中如何搜索已加密邮件和授权他人处理已加密邮件的问题，提出一种面向电子邮件系统支持关键字搜索的代理重加密方案。利用可搜索加密技术对加密邮件进行搜索，使用代理重加密技术对加密邮件授权。安全性证明及效率分析结果表明，该方案可以更好地抵抗篡改攻击和关键字离线猜测攻击，同时，在标准模型下，证明了该方案在判定 Diffie-Hellman 问题、双线性判定 Diffie-Hellman 问题、商判定 Bilinear Diffie-Hellman 问题上，分别满足陷门隐私安全、关键字隐私安全和密文隐私安全。相比 dPRES 方案，该方案减少了时间开销，提高了搜索效率和解密效率。

关键词： 代理重加密；关键字搜索；电子邮件；Diffie-Hellman 问题；双线性判定 Diffie-Hellman 问题；商判定 Bilinear Diffie-Hellman 问题

开放科学（资源服务）标志码（OSID）：

中文引用格式： 牛淑芬，陈俐霞，刘文科，等. 电子邮件系统中支持关键字搜索的代理重加密方案[J]. 计算机工程，2020，46(6)：136-143.

英文引用格式： NIU Shufen，CHEN Lixia，LIU Wenke，et al. Proxy re-encryption scheme supporting keyword search in email system[J]. Computer Engineering，2020，46(6)：136-143.

Proxy Re-Encryption Scheme Supporting Keyword Search in Email System

NIU Shufen[a]，CHEN Lixia[a]，LIU Wenke[a]，WANG Caifen[a]，DU Xiaoni[b]

（a. College of Computer Science and Engineering；b. College of Mathematics and Statistics，
Northwest Normal University，Lanzhou 730070，China）

【Abstract】 To authorize others to deal with encrypted mails and enable the search of encrypted mails in an encrypted email system，this paper proposes a proxy re-encryption scheme that supports keyword search for email systems. In this scheme，searchable encryption technology is used to search encrypted mails，and then proxy re-encryption technology is used to authorize encrypted mails. Security certification and efficiency analysis results show that the proposed scheme can better resist tampering attacks and keyword offline guessing attacks. At the same time，under the standard model，it is proven that the scheme respectively meets trapdoor privacy security，keyword privacy security and ciphertext privacy security in the determination of the Diffie-Hellman problem，the Decisional Bilinear Diffie-Hellman（DBDH）problem，and the Quotient Decisional Bilinear Diffie-Hellman（QDBDH）problem. Compared with the dPRES scheme，the proposed scheme reduces the time cost and improves the efficiency of search and decryption.

【Key words】 Proxy Re-Encryption（PRE）；keyword search；email；Diffie-Hellman problem；Decisional Bilinear Diffie-Hellman（DBDH）problem；Quotient Decisional Bilinear Diffie-Hellman（QDBDH）problem

DOI： 10.19678/j.issn.1000-3428.0055554

0 概述

在电子邮件系统中，当数据发送者发给用户的邮件因用户的私人原因而无法及时处理时，用户希望将该邮件共享给被委托者，并由对方帮助其处理该邮件。一般情况下，用户先下载某个邮件，用其私钥解密该邮件并使用被委托者的公钥进行加密处理，最后发送给被委托者，该方式需要较大的计算代价和通信代价，而代理重加密（Proxy Re-Encryption，PRE）技术可有效解决这一问题。

基金项目： 国家自然科学基金（61562077，61662071，61662069，61772022）。

作者简介： 牛淑芬（1976—），女，副教授，主研方向为大数据网络隐私保护、云计算；陈俐霞、刘文科，硕士研究生；王彩芬、杜小妮，教授。

收稿日期： 2019-07-22 **修回日期：** 2019-08-30 **E-mail：** sfniu76@nwnu.edu.cn

1998 年,BLAZE 等人[1]提出 PRE 的概念,主要内容是委托者通过一个半可信的代理者将密文授权给被委托者,且在这个过程中,代理者得不到消息的任何信息。文献[2]提出一个单向的 PRE 方案,但是该方案只能达到选择明文安全的要求,文献[3]提出第一个满足 IND-CCA2 的双向 PRE 方案。文献[4]在文献[5]的基础上,改进了方案的安全模型,并构造一个安全的 IND-CCA2 单向的 PRE 方案。文献[6]提出多跳 PRE 方案,同年,文献[7]提出电子病历中带关键字搜索的公钥加密方案。为解决复杂证书问题和密钥管理问题,文献[8]提出新的基于证书条件的 PRE 方案。文献[9]构造管理云端数据访问授权确定性更新的 PRE 方案。为解决云端数据共享问题,文献[10]提出标准模型下 CPA 安全的格上 PRE 方案。

随着电子邮件服务器上数据的增加,为了实现密文搜索和数据共享 2 个功能,文献[11]提出带关键字搜索的 PRE 的概念,且构造在随机预言模型下可证明安全的 PRES 方案,但文献[12]指出文献[11]存在使用了一次性强不可伪造签名来保证方案安全性的限制。文献[13]构造出有效且不使用一次性强不可伪造签名的 PRE 方案,并证明该方案可使选择密文安全。为提高方案的效率,文献[14]依据文献[11,15]构造出只对部分文件的密文进行重加密的方案模型。为抵抗由不可信服务器执行的关键字猜测攻击,文献[16]提出新的支持关键字搜索的加密方案,文献[17]提出基于关键字搜索属性的 PRE 方案。

现有的支持关键字搜索的 PRE 方案存在一些问题需要解决,如抵抗关键字猜测攻击和数据篡改等。在文献[18-19]中,验证等式的信息都是公开信息或对方发送的信息,易遭受篡改攻击。针对这一问题,本文提出在加密电子邮件背景下支持关键字搜索的 PRE 方案。在该方案中,服务器、邮箱网关与被委托者的验证方式均不同,并且其采用更加高效的对称加密方式,以提高搜索效率和解密效率。

1　基础知识

1.1　双线性对

令$(G_1,+)$和$(G_2,\times)$是阶为素数 p、q 的循环群,双线性映射 $e:G_1\times G_1\to G_2$ 满足以下性质:

1)双线性:对任意的 $P,Q\in G_1$,存在 $a,b\in Z_q^*$,有 $e(aP,bQ)=e(P,Q)^{ab}$成立。

2)非退化性:存在 $P,Q\in G_1$,满足 $e(P,Q)\neq 1$。

3)可计算性:对于任意的 $P,Q\in G_1$,存在有效的算法计算 $e(P,Q)$。

1.2　相关的困难问题

1)判定 Diffie-Hellman(Decisional Diffie-Hellman,DDH)问题。

给定一个四元组(g,g^a,g^b,g^c),其中随机取 a,$b,c\in Z_p^*$,g 为群 G_1 的一个生成元,判定 $g^c=g^{ab}$是否成立。

2)双线性判定 Diffie-Hellman(Decisional Bilinear Diffie-Hellman,DBDH)问题。

给定一个五元组(g,g^a,g^b,g^c,r),其中随机取 $a,b,c\in Z_p^*$,且 $r\in G_2$,g 为 G_1 群的一个生成元,判定 $r=e(g,g)^{abc}$是否成立。

3)商判定 Bilinear Diffie-Hellman(Quotient Decisional Bilinear Diffie-Hellman,QDBDH)问题。

给定一个四元组(g,g^a,g^b,r),其中随机取 $a,b,c\in Z_p^*$,且 $r\in G_2$,g 为 G_1 群的一个生成元,判定 $r=e(g,g)^{\frac{b}{a}}$是否成立。

2　方案模型和安全模型

2.1　方案摸型

本节提出面向电子邮件高效支持关键字搜索的 PRE 方案。本方案实现了密文授权和密文搜索的功能,具体如下:邮件发送者将已加密的邮件发送给用户 i,而用户 i 希望将该邮件授权给用户 j 处理,便由加密邮箱服务器作为代理者对密文进行重加密,将邮箱网关搜索重加密邮件密文,并发送给用户 j 解密。该方案包括如下算法:

1)Setup(l):输入安全参数 1^l,输出系统参数 Params。

2)KeyGen(Params):输入系统参数 Params,输出用户和加密邮箱服务器 S 的公私钥对。

3)ReKeyGen(X_i,X_j):输入用户 i 的私钥 X_i 和用户 j 的私钥 X_j,加密邮箱服务器 S 生成重加密密钥 $RK_{i\to j}$。

4)Enc(Y_i,Y_S,w,m):输入用户 i 的公钥 Y_i、加密邮箱服务器 S 的公钥 Y_S、关键字 w 和明文 $m\in\{0,1\}^*$,输出基于用户 i 公钥的密文 CT_i。

5)ReEnc(CT_i,Y_i,X_S):输入基于用户 i 公钥的密文 CT_i、用户 i 的公钥 Y_i、加密邮箱服务器 S 的私钥 X_S、重加密密钥 $RK_{i\to j}$,加密邮箱服务器 S 输出基于用户 j 公钥的密文 CT_j。

6)Trapdoor(X_j,Y_s,w,CT_j):输入用户 j 的私钥 X_j、加密邮箱服务器 S 的公钥 Y_S、基于用户 j 公钥的密文 CT_j 和关键字 w,用户 j 生成陷门 T。

7)Test(CT_j,T):输入基于公钥的密文 CT_j 和关键字陷门 T,邮件网关通过算法 Test(CT_j,T)验证陷门与密文是否匹配。若陷门与密文相匹配,邮件网关发送基于用户 j 公钥的密文给用户 j,否则,邮箱网关输出 $\perp$。

8)Dec(CT_j):输入密文 CT_j 和私钥 X_j,用户 j 输出明文 m。

2.2 安全模型

在标准模型下,本文方案满足关键字密文隐私安全和陷门隐私安全[20-22]。

2.2.1 关键字密文隐私安全

为满足关键字密文的不可区分性,本文方案考虑敌手 $A_i(i=1,2)$ 和挑战者 B 之间的 2 个游戏。

游戏 1 该游戏的目的是证明密文的不可区分性。在游戏中,本文方案假设敌手 A_1 是恶意的邮箱服务器。

系统建立 挑战者 B 产生公共参数并将其给敌手 A_1。

询问阶段 1 敌手 A_1 进行如下询问:

1)公钥预言询问 $O_{Y_i}(i)$:挑战者 B 模拟算法 KeyGen 产生公私钥对 (Y_i,X_i) 并将公钥 Y_i 公开;敌手 A_1 模拟算法 KeyGen 产生它的公私钥对 (Y_j,X_j) 并将公钥 Y_j 公开。

2)重加密密钥询问阶段 $O_{RK}(X_i,X_j)$:挑战者 B 模拟 ReKeyGen 算法产生重加密密钥 $RK_{i\to j}$ 并输出给敌手 A_1。

3)重加密预言阶段 $O_{\mathrm{Re}}(Y_i,Y_j,CT_i)$:挑战者 B 模拟重加密算法生成基于被委托者公钥的密文 CT_j 并将其发送给敌手 A_1。

4)陷门预言阶段 $O_T(w,X_j)$:敌手进行询问,挑战者 B 则回应相对应的陷门。

5)解密预言阶段 $O_{\mathrm{Dec}}(Y_i,CT_j)$:挑战者 B 输出 $\mathrm{Dec}(CT_j)$ 给敌手 A_1。

挑战 当询问阶段 1 完毕,敌手 A_1 选择 2 个明文 (m_0,m_1) 发送给挑战者 B。挑战者 B 随机选取 $\delta\in\{0,1\}$,并设置嵌入困难问题的挑战密文发送给敌手 A_1。

询问阶段 2 除了不能询问挑战密文及其衍生外,其他询问同询问阶段 1 一致。

猜测 敌手返回猜测 δ',如果 $\delta'=\delta$,则敌手猜测成功,输出 1,否则,输出 0。游戏 1 中的优势定义为 $\mathrm{Adv}_{A_1}^{\mathrm{Game1}}(k)=\left|\Pr[\delta=\delta']-\frac{1}{2}\right|$。

游戏 2 该游戏的目的是证明关键字的不可区分性。在游戏中,本文方案假设敌手 A_2 是外部攻击者,在游戏中,挑战者 B 和敌手 A_2 进行如下交互:

系统建立 挑战者 B 产生公共参数并将其给敌手 A_2。

询问阶段 1 重复游戏 1 中的询问阶段 1。

挑战 当询问阶段 1 结束,敌手 A_2 选择 2 个关键字 (w_1,w_2)、明文 m 和公钥 Y^* 一起发送给挑战者 B。挑战者 B 随机选择 $\delta\in\{0,1\}$,并设置嵌入困难问题的挑战密文发送给敌手 A_2。

询问阶段 2 敌手 A_2 进行询问时,除了不能询问挑战密文及其衍生外,其他询问同询问阶段 1 一致。

猜测 敌手返回猜测 δ',如果 $\delta'=\delta$,则挑战成功,输出 1,否则,输出 0。游戏 2 中的优势定义为 $\mathrm{Adv}_{A_2}^{\mathrm{Game2}}(k)=\left|\Pr[\delta=\delta']-\frac{1}{2}\right|$。

2.2.2 陷门隐私安全

为了抵抗关键字猜测攻击,文献[12]引入了陷门不可区分性。

游戏 3 假设敌手 A_3 是外部攻击者,在游戏中,挑战者 B 和敌手 A_3 进行如下交互:

系统建立 挑战者 B 产生公共参数并公开。

询问阶段 1 敌手 A_3 对关键字 w 进行陷门询问,挑战者 B 回应陷门。

挑战阶段 敌手 A_3 选择 2 个关键字 (w_1,w_2)、明文 m 和公钥 Y^* 一起发送给挑战者 B。挑战者 B 随机选取 $\delta\in\{0,1\}$,并计算陷门发送给敌手 A_3。

询问阶段 2 除了不能询问挑战关键字及其衍生外,其他询问同询问阶段 1 一致。

猜测 敌手返回猜测 δ',如果 $\delta'=\delta$,则挑战成功,输出 1,否则,输出 0。游戏 3 中的优势定义为 $\mathrm{Adv}_{A_3}^{\mathrm{Game3}}(k)=\left|\Pr[\delta=\delta']-\frac{1}{2}\right|$。

3 方案设计

3.1 方案构造

本文提出的方案包括 8 个部分,具体设计如下:

1)$\mathrm{Setup}(I)$:输入安全参数 I^l,输出阶为素数 p 的循环加法群 G_1 和循环乘法群 G_2,g 为群 G_1 的生成元,g_2,u,v,d 是群 G_1 上的随机元,双线性映射对 $e:G_1\times G_1\to G_2$。方案构造 2 个散列函数:$H_1:G_1\times\{0,1\}^*\times\{0,1\}^L\to Z_p^*$,$H_2:G_2\to\{0,1\}^L$,$L$ 为对称密钥 K 的长度,则系统参数 $\mathrm{Params}=\{P,G_1,G_2,e,g,g_1,u,v,d,H_1,H_2,K\}$。

2)$\mathrm{KeyGen}(\mathrm{Params})$:输入系统参数 Params,用户 i 随机选择 $X_i\in Z_p^*$,并计算 $Y_i=g^{X_i}$,则公私钥对为 (X_i,Y_i)。加密邮箱服务器 S 随机选取 $X_S\in Z_p^*$,计算 $Y_S=g^{X_S}$ 作为加密邮箱服务器 S 的公钥。

3)$\mathrm{ReKeyGen}(X_i,X_j)$:输入用户 i 的私钥 X_i 和用户 j 的私钥 X_j,生成重加密密钥 $RK_{i\to j}=\frac{X_j}{X_i}\bmod p$。具体操作如下:

(1)用户 i 选取 $r'\in Z_p^*$,并发送 $r'\cdot X_i\bmod p$ 给用户 j,同时发送 r' 给加密邮箱服务器 S。

(2)用户 j 计算 $\frac{X_j}{r'X_i}$ 并发送给加密邮箱服务器 S。

(3)利用加密邮箱服务器 S 计算 $RK_{i\to j}=r'\cdot\frac{X_j}{r'X_i}=\frac{X_j}{X_i}\bmod p$ 作为 PRE 密钥。

4)$\mathrm{Enc}(Y_i,Y_S,w,m)$:输入用户 i 的公钥 Y_i、加密邮箱服务器 S 的公钥 Y_S、关键字 w 和明文 $m\in\{0,1\}^*$,用户 i 进行如下操作:

(1)选取 $r\in Z_p^*$,计算 $A=g^r$,$B=Y_i^r$,用对称加密算法计算 $C=\mathrm{Enc}_K(m)$。

(2)计算 $D=e(Y_s,g_2^w)^r$,$E=H_2(e(g,g)^r)\oplus K$。

(3)随机选取 $t \in Z_p^*$,计算 $h = H_1(A, C, E)$, $D_1 = e(g, g_2^w h)^r$, $F = (u^h v^t d)^r$, $G = g_2^{rw}$。

(4)输出基于用户 i 公钥的密文 $CT_i = (t, A, B, C, D, D_1, E, F, G)$。

5) ReEnc(CT_i, Y_i, X_S):输入密文 CT_i、用户 i 的公钥 Y_i、加密邮件服务器 S 的私钥 X_S 和重加密密钥 $RK_{i\to j}$,邮件服务器 S 计算 $h = H_1(A, C, E)$,并验证式(1)是否成立:

$$D^{\frac{1}{X_S}} e(A, Y_i (u^h v^t d)) = e(g, B \cdot F \cdot G) \tag{1}$$

若式(1)成立,利用加密邮件服务器 S 计算 $B' = B^{RK_{i\to j}} = Y_j^r$,输出基于用户 j 公钥的密文 $CT_j = (t, A, B', C, D, D_1, E, F, G)$;否则输出 $\perp$。

6) Trapdoor(X_j, Y_s, w, CT_j):输入用户 j 的私钥 X_j、加密邮件服务器 S 的公钥 Y_S、基于用户 j 公钥的密文 CT_j 和关键字 w,用户 j 计算 $h = H_1(A, C, E)$,从而得到陷门 $T = (g_2^w h)^{\frac{1}{X_j}}$。

7) Test(CT_j, T):输入基于用户 j 公钥的密文 $CT_j = (t, A, B', C, D, D_1, E, F, G)$ 和关键字 w 的陷门 T,加密邮件网关验证式(2)是否成立:

$$e(B', T) = D_1 \tag{2}$$

若式(2)成立,用加密邮件网关将基于用户 j 公钥的密文 CT_j 发送给用户 j;否则输出 $\perp$。

8) Dec(CT_j):输入密文 CT_j,用户 j 计算 $h = H_1(A, C, E)$,并验证式(3)是否成立:

$$e(B', g)^{\frac{1}{X_j}} = e(g, A) \tag{3}$$

若式(3)成立,用户 j 通过式(4)计算对称密钥 K',则明文 $m = \mathrm{Dec}_{K'}(C)$;否则输出 $\perp$。

$$K' = E \oplus H_2(e(B', g)^{\frac{1}{X_j}}) \tag{4}$$

3.2　正确性证明

本文方案满足正确性。在重加密过程中,邮件服务器验证式(1)是为了证明密文 CT_i 在传输过程中并没有被篡改。在搜索过程中,加密邮件网关通过验证式(2)来实现关键字与密文之间的匹配。在解密过程中,用户 j 通过式(3)验证重加密密文是否被篡改,通过式(4)解密密文。验证过程如下:

1) $D^{\frac{1}{X_S}} e(A, Y_i (u^h v^t d)) =$

$e(Y_S, g_2^w)^{\frac{1}{X_S}} e(g^r, Y_i (u^h v^t d)) =$

$e(g, g_2^w)^r e(g^r, Y_i (u^h v^t d)) = e(g^r, g_2^w Y_i (u^h v^t d)) =$

$e(g, g_2^{wr} g^{X_j r} (u^h v^b d)^r) = e(g, B \cdot F \cdot G)$

2) $e(B', T) = (Y_j^r, (g_2^w h)^{\frac{1}{X_j}}) = e(g^{X_j r}, (g_2^w h)^{\frac{1}{X_j}}) =$

$e(g^r, g_2^w h) = e(g, g_2^w h)^r = D_1$

3) $e(B', g)^{\frac{1}{X_j}} = e(g^{X_j r}, g)^{\frac{1}{X_j}} = e(g, A)$

4) $K' = E \oplus H_2(e(B', g)^{\frac{1}{X_j}}) =$

$H_2(e(g, g)^r) \oplus K \oplus H_2(e(g^{rX_j}, g)^{\frac{1}{X_j}}) = K$

因此本文方案是正确的。

4　安全性证明

4.1　关键字密文隐私安全

定理 1　假设解决 QDBDH 和 DBDH 问题困难,本文方案在标准模型下可证明 IND-CCA 和 IND-CKA 是安全的。

引理 1　假设解决 QDBDH 问题困难,本文方案在标准模型下可证明 IND-CCA 是安全的。

证明　假设存在恶意的邮箱服务器 A_1 能以优势 ε 攻破本文方案($q_{RK}, q_{RE}, q_T, q_{\mathrm{Dec}}, \varepsilon$),则挑战者 B 便能以不可忽略的优势解决 QDBDH 问题。设 H_1、H_2、H_3 是免碰撞的哈希函数,且 K 是对称加密密码。则有 $\varepsilon \geqslant \frac{\varepsilon}{e(1+q_{RK})} - \frac{q_{RE}+q_{\mathrm{Dec}}}{p} - \mathrm{Adv}_{H,A_1}^{\mathrm{TCR}} - \mathrm{Adv}_K^{\mathrm{PRF}}$。

假设给挑战者 B 一个 QDBDH 实例($g, M = g^a, N = g^b, Q$) $\in (G_1)^3 \times G_2$,其中 $a, b \in Z_p^*$,挑战者 B 的目的是确定 $Q = e(g, g)^{\frac{b}{a}}$ 是否成立。游戏过程如下:

系统建立　挑战者 B 选取随机数 $a_0, a_1, a_2, a_3, b_1, b_2, b_3$,计算系统参数 $g_2 = M^{a_0}$, $h = M^b$, $u = g^{a_1} N^{b_1}$, $v = g^{a_2} N^{b_2}$, $d = g^{a_3} N^{b_3}$。

询问阶段 1　敌手 A_1 进行如下询问:

1)公钥预言询问 $O_{Y_i}(i)$:挑战者 B 随机选取 $X_i \in Z_p^*$,并抛掷一个硬币,若正面朝上,则 $c_i = 1$,公钥 $Y_i = g^{X_i}$;否则 $c_i = 0$,公钥 $Y_i = g^{aX_i} = M^{X_i}$。挑战者 B 将三元组(Y_i, X_i, c_i)加入至列表 L^{list} 中并将公钥 Y_i 公开。敌手 A_1 产生它的公私钥对(Y_j, X_j)并将公钥 Y_j 公开。

2)重加密密钥询问阶段 $O_{RK}(X_i, X_j)$:从列表 L^{list} 中调用三元组(Y_i, X_i, c_i),并查询 X_i 和 X_j 是否存在三元组中,若不存在,则调用公钥预言询问 $O_{Y_i}(i)$,否则进行如下操作:

(1)若 $c_i = c_j = 1$,则用户 i 的私钥为 X_i,用户 j 的私钥为 X_j,挑战者 B 模拟算法 ReKeyGen(X_i, X_j)产生代理重加密密钥 $RK_{i\to j} = \frac{X_j}{X_i}$。

(2)若 $c_i = c_j = 0$,则用户 i 的私钥为 aX_i,用户 j 的私钥为 aX_j,挑战者 B 模拟算法 ReKeyGen(X_i, X_j)产生 PRE 密钥 $RK_{i\to j} = \frac{aX_j}{aX_i} = \frac{X_j}{X_i}$。

(3)否则,挑战者 B 输出 $\perp$。

3)陷门预言阶段 $O_T(w, X_j)$:挑战者 B 从列表 L^{list} 中调用三元组(Y_i, X_i, c_i)并查询 X_j 是否存在三元组中,若不存在,则调用公钥预言询问 $O_{Y_i}(i)$,否则进行如下操作:

(1)若 $c_j = 1$,则用户 j 的私钥为 X_j,挑战者 B 设陷门为 $T = g^{\frac{aa_0 w}{X_j}} g^{\frac{b}{X_j}} = (g_2^w h)^{\frac{1}{X_j}}$。

(2)若 $c_j=0$,则用户 j 的私钥为 aX_j,挑战者 B 设陷门为 $T=g^{\frac{a_0w}{X_j}}g^{\frac{b}{X_j}}=(g_2^wh)^{\frac{1}{aX_j}}$。

4)重加密预言阶段 $O_{RE}(Y_i,Y_j,CT_i)$:若式(1)验证失败,则挑战者 B 输出 $\perp$;否则挑战者 B 从列表 L^{list} 中恢复三元组(Y_i,X_i,c_i)并执行如下操作:

(1)若 c_i 和 c_j 均为 1 或均为 0,则挑战者 B 调用重加密密钥询问 $O_{RK}(X_i,X_j)$,生成重加密密钥 $RK_{i\to j}$,然后将 $\mathrm{ReEnc}(CT_i,RK_{i\to j})$返回给敌手 A_1。

(2)若 $c_i=0\wedge c_j=1$,则意味着用户 i 的私钥为 X_i 和用户 j 的私钥为 aX_j,挑战者 B 通过 $A=g^r=M^{\frac{r}{a}}$ 和 $F=(u^hv^td)^r=(g^{a_1h+a_2t+a_3}M^{b_1h+b_3t+b_3})$计算:

$$g^r=\left[\frac{F}{M^{a(b_1h+b_3t+b_3)}}\right]^{\frac{1}{a_1h+a_2t+a_3}} \tag{5}$$

则通过式(5)得到 $B'=(g^r)^{X_j}=Y_j^r$,并将 $CT_j=(t,A,B',C,D,D_1,E,F,G)$ 发送给敌手 A_1,等式 $a_1h+a_2t+a_3=o\bmod p$ 至少以$\frac{1}{p}$的概率成立。

(3)若 $c_i=1\wedge c_j=0$,则意味着用户 i 的私钥为 aX_i 和用户 j 的私钥为 X_j,挑战者 B 计算 $B'=g^{aX_jr}=(M^r)^{X_j}=A^{aX_j}$。

5)解密预言阶段 $O_{\mathrm{Dec}}(Y_i,CT_j)$:挑战者 B 从列表 L^{list} 中恢复三元组(Y_i,X_i,c_i)并执行如下操作:

(1)若 $c_j=0$,则用户 j 的私钥为 aX_j,挑战者 B 验证式(3),若式(3)验证失败,则挑战者 B 输出 $\perp$;否则挑战者 B 计算对称密码 $K=E\oplus H_2(e(B',g)^{\frac{1}{aX_j}})=E\oplus H_2(e(g,g)^r)$,然后计算得到 $m=\mathrm{Dec}_{K'}(C)$。

(2)若 $c_j=1$,则用户 j 的私钥为 X_j,挑战者 B 将输出 $\mathrm{Dec}(CT_j)$给敌手。

挑战阶段 当询问阶段 1 完毕,敌手 A_1 选择 2 个明文(m_0,m_1)、公钥 Y^* 一起发送给挑战者 B。挑战者 B 从列表 L^{list} 中恢复三元组(Y_i,X_i,c_i),若 $c^*=1$,挑战者 B 输出 $\perp$,否则挑战者 B 随机选取 $\delta\in\{0,1\}$,并设置 $A^*=N^{\frac{1}{a}}$,$B^*=N^{\frac{X_j^*}{a}}$,$C^*=\mathrm{Enc}_{K^*}(m_\delta)$,$D^*=e(Y_s,N^{a_0w})$,$h^*=H_1(A^*,C^*,E^*)$,$t^*=-\dfrac{a_1h^*+a_3}{a_2}$,$F^*=N^{b_1h^*+b_2t^*+b_3}$,$G^*=N^{a_0w}$。挑战者 B 输出挑战密文 $CT_i^*=(t,A^*,B^*,C^*,D^*,D_1^*,E^*,F^*,G^*)$给敌手 A_1。

如果 $Q=e(g,g)^{\frac{b}{a}}$,CT_i^* 是基于公钥 Y^* 下的挑战密文,设 $r^*=\dfrac{b}{a}$,则有 $A^*=N^{\frac{1}{a}}=(g)^{\frac{b}{a}}=g^{r^*}$,$B^*=N^{\frac{X_j^*}{a}}=g^{\frac{bX_j^*}{a}}=(g^{X_j^*})^{r^*}$,$C^*=\mathrm{Enc}_{K^*}(m_\delta)$,$D^*=e(Y_s,N^{a_0w})=e(Y_s,g^{aa_0w})^{\frac{b}{a}}=e(Y_s,g_2^w)^{r^*}$,$D_1^*=e(g,N^{a_0w}N^b)=e(g,M^{a_0w}M^b)^{r^*}=e(g,g_2^wh)^{r^*}$,$E^*=H_2(e(g,N^{\frac{1}{a}}))\oplus K^*=H_2(e(g,g)^{r^*})\oplus K^*$,$F^*=N^{b_1h^*+b_2t^*+b_3}=(g^{a_1h^*+a_3+a_2t^*}M^{b_1h^*+b_2t^*+b_3})^{r^*}$,$G^*=N^{a_0w}=(A^{a_0w})^{r^*}=(g_2^w)^{r^*}$。

询问阶段 2 敌手 A_1 进行询问,除了挑战密文及其衍生不能询问外,其他与询问阶段 1 一致。

猜测 最后敌手返回猜测 δ',如果 $\delta'=\delta$,则挑战成功,输出 1;否则输出 0。

引理 2 假设解决 DBDH 问题困难。本文方案在标准模型下可证明 IND-CKA 是安全的。

证明 假设敌手 A_2 是外部攻击者,其以优势 ξ 攻破本文方案$(q_{RK},q_{RE},q_T,q_{\mathrm{Dec}},\xi)$,则本文方案能够构造挑战者 B 以一个不可忽略的优势解决 DBDH 问题。若 H_1,H_2,H_3 是免碰撞的哈希函数,且 K 是对称加密密码,则有 $\xi\geqslant\dfrac{\varepsilon}{e(1+q_{RK})}-\dfrac{q_{RE}+q_{\mathrm{Dec}}}{p}-\mathrm{Adv}_{H,A_1}^{\mathrm{TCR}}-\mathrm{Adv}_K^{\mathrm{PRF}}$。

假设给挑战者 B 一个 DBDH 实例$(g,M=g^a,N=g^b,O=g^c,\gamma)\in(G_1)^3\times G_2$,其中 $a,b,c\in Z_p^*$,挑战者 B 的目的是确定 $\gamma=e(g,g)^{abc}$ 是否成立。游戏过程如下:

系统建立 挑战者 B 随机选取数 a_0,a_1,a_2,a_3,b_1,b_2,b_3,计算系统参数 $g_2=M^{a_0}$,$h=M^b$,$u=g^{a_1}N^{b_1}$,$v=g^{a_2}N^{b_2}$,$d=g^{a_3}N^{b_3}$。

询问阶段 1 敌手 A_2 进行如下询问:

1)公钥预言询问 $O_{Y_i}(i)$:挑战者 B 随机选取 $X_i\in Z_p^*$,并计算公钥 $Y_i=g^{X_i}$。

2)重加密密钥询问阶段 $O_{RK}(X_i,X_j)$:挑战者 B 生成代理重加密密钥 $RK_{i\to j}=\dfrac{X_j}{X_i}$。

3)陷门预言阶段 $O_T(w,X_j)$:挑战者 B 生成陷门 $T=(g_2^wh)^{\frac{1}{X_j}}$。

4)重加密预言阶段 $O_{RE}(Y_i,Y_j,CT_i)$:若式(1)验证失败,则挑战者 B 输出 $\perp$;否则挑战者 B 调用重加密密钥询问 $O_{RK}(X_i,X_j)$,生成重加密密钥 $RK_{i\to j}=\dfrac{X_j}{X_i}$,并将 $\mathrm{ReEnc}(CT_i,RK_{i\to j})$返回给敌手 A_2。

5)解密预言阶段 $O_{\mathrm{Dec}}(Y_i,CT_j)$:挑战者 B 输出 $\mathrm{Dec}(CT_j)$给敌手 A_2。

挑战阶段 当询问阶段 1 完毕,敌手 A_2 选择 2 个关键字(w_0,w_1)、明文 m 和公钥 Y^* 一起发送给挑战者 B。挑战者 B 随机选取 $\delta\in\{0,1\}$,并设置 $r^*=c$ 为 DBDH 困难问题里的成分,计算 $A^*=O$,$B^*=$

$O^{X_j*}, C^* = \mathrm{Enc}_{K^*}(m), D^* = e(Y_s, O^{a_0 aw}), E^* = H_2(e(g,O)) \oplus K^*\ h^* = H_1(A^*, C^*, E^*), F^* = O^{a_1 h^* + a_2 t^* + a_3}, G^* = O^{a_0 aw}, D_1{}^* = \gamma^{\left(\frac{a_0 w}{b}+1\right)}$。挑战者 B 将挑战密文 $CT_i{}^* = (t, A^*, B^*, C^*, D^*, D_1{}^*, E^*, F^*, G^*)$返回给敌手 A_2。若 $\gamma = e(g,g)^{abc}$, $CT_i{}^*$ 是基于公钥 Y^* 下的挑战密文,则有 $A^* = O = g^c = g^{r^*}, B^* = O^{X_j*} = g^{cX_j*} = Y_j^{r^*}, D_1{}^* = \gamma^{\left(\frac{a_0 w}{b}+1\right)} = e(g, g^{a_0 aw} g^{ab})^{r^*} = e(g, g_2^w h)^{r^*}$。

询问阶段 2　敌手 A_2 进行询问,除了挑战密文及其衍生不能询问外,其他同询问阶段 1 一致。

猜测　敌手返回猜测 δ',若 $\delta' = \delta$,则挑战成功,输出 1;否则输出 0。

4.2　陷门隐私安全

定理 2　假设解决 DDH 问题困难。本文方案可证明在陷门上是安全的。

证明　假设存在外部攻击者 A_3 能以优势 ζ 攻破本文方案$(q_{RK}, q_{RE}, q_{\mathrm{Dec}}, \zeta)$,则存在挑战者 B 能以优势 ζ 解决 HDH 问题。假设 H_1、H_2、H_3 是免碰撞的哈希函数,且 K 是对称加密密码,敌手询问陷门的次数为 q_T 次,其中 $\zeta \geqslant \frac{\varepsilon'}{e(1+q_{RK})} - \frac{q_{RE}+q_{\mathrm{Dec}}}{p} - \mathrm{Adv}^{\mathrm{TCR}}_{H.A_1} - \mathrm{Adv}^{\mathrm{PRF}}_{K}$ 成立。

假设给挑战者 B 一个 HDH 实例$(g, M = g^a, N = g^b, \lambda) \in G_1$,其中 $a, b \in Z_p^*$,挑战者 B 的目的是确定 $\lambda = g^{ab}$是否成立。游戏过程如下:

系统建立　挑战者 B 选取随机数 a_0、a_1、a_2、a_3、b_1、b_2、b_3、并计算系统参数 $g_2 = M^{a_0}, h = M^b$。

询问阶段 1　敌手 A_3 进行如下询问:

1)公钥预言询问 $O_{Y_i}(i)$:挑战者 B 随机选择 $X_i \in Z_p^*$。并抛掷一个硬币,若正面朝上,则 $c_i = 1$,公钥 $Y_i = g^{X_i}$;否则 $c_i = 0$,公钥 $Y_i = g^{aX_i} = N^{X_i}$。挑战者 B 将三元组(Y_i, X_i, c_i)加入到列表 L^{list}中,将私钥 X_i 返回给敌手 A_1,公开公钥 Y_i。

2)陷门预言阶段 $O_T(w, X_j)$:挑战者 B 从列表 L^{list}中调用三元组(Y_i, X_i, c_i)并查询 X_j 是否存在三元组中,若不存在,则调用公钥预言询问 $O_{Y_i}(i)$,否则进行如下操作:

1)若 $c_j = 1$,则用户 j 的私钥为 X_j,挑战者 B 设陷门为 $T = g^{\frac{a_0 abw}{X_j}} g^{\frac{b}{X_j}} = (g_2^w h)^{\frac{1}{X_j}}$。

2)若 $c_j = 0$,则用户 j 的私钥为 aX_j,挑战者 B 设陷门为 $T = g^{\frac{a_0 bw}{X_j}} g^{\frac{b}{X_j}} = (g_2^w h)^{\frac{1}{aX_j}}$。

挑战阶段　敌手 A_3 选择 2 个关键字(w_0, w_1),并发送给挑战者 B。挑战者 B 从列表 L^{list}中恢复三元组(Y_i, X_i, c_i),若 $c^* = 1$,则挑战者 B 输出 $\perp$;若 $c^* = 0$,则挑战者 B 随机选择 $\delta \in \{0,1\}$,并生成挑战陷门 $T^* = \lambda^{\frac{a_0 w_\delta}{X_j*}}$,其中 λ 是 DDH 困难问题中的成分。若 $\lambda = g^{ab}$, $T^* = \lambda^{\frac{a_0 w_\delta + 1}{X_j*}} = g^{\frac{a_0 abw_\delta + ab}{X_j*}} = M^{\frac{a_0 bw_\delta + b}{X_j*}} = (g_2^{w_\delta} h)^{\frac{1}{X_j*}}$均成立,则 T^* 是公钥 Y_j 下的一个有效陷门。

询问阶段 2　敌手 A_3 进行询问,除了不能询问挑战关键字及其衍生外,其他同询问阶段 1 一致。

猜测　敌手 A_3 返回猜测 δ',若 $\delta' = \delta$,则挑战成功,输出 1;否则输出 0。

5　效率分析

通过理论和数值实验对 dPRES[18] 方案和本文方案进行分析。首先从理论上对计算开销进行分析,dPRES 方案和本文方案效率比较结果见表 1,其中 T_p、T_F、T_h、T_e、T_{eo}分别为双线性运算、伪随机函数族运算、哈希运算、指数运算和异或运算的计算代价。

表 1　dPRES 方案与本文方案的效率比较

Table 1　Comparison of the efficiency of dPRES scheme and the proposed scheme

方案	加密	重加密	搜索	解密	安全性
dPRES 方案	$T_p + 5T_e + T_h + T_F$	$2T_p + T_e$	$T_p + T_e + 2T_h$	$3T_p + T_e + T_F$	CCA
本文方案	$3T_p + 4T_e + T_h + T_{eo}$	$2T_p + T_e$	T_p	$2T_p + T_h + T_{eo}$	CCA

由表 1 可知,在搜索阶段,本文方案比 dPRES 方案少一个指数运算和两个哈希运算。此外,在解密阶段,本文方案比 dPRES 方案少一个双线性对运算。因此,与 dPRES 方案相比,本文方案在计算效率上有较大的提高。

为了更直观地显示结果,本节从数值分析上对方案的计算成本进行了模拟。在 Linux 系统上使用 PBC 库,基于 C 语言编程实现 dPRES 方案和本方案。数值环境配置参数如表 2 所示。

表 2　环境配置参数

Table 2　Environmental configuration parameters

环境配置	参数
电脑型号	Lenovo y485p
操作系统	Windows 10
处理器	AMD A10-5750M APU with Radeon(tm)HD Graphics. 2.50 GHz
内存	4 GB
虚拟机	Linux

本文方案和 dPRES 方案均能实现密文授权和搜索功能。在数值实验中,加密和解密阶段两方案均加密相同数量的关键字,随着关键字数量的变化,统计在不同数量关键字下的加密时间,结果如图 1 所示。

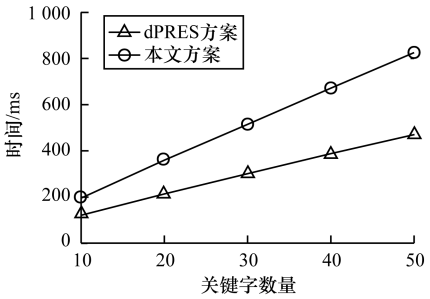

图 1 关键字数量对加密时间的影响

Fig. 1 Effect of the number of keywords on encryption time

由图 1 可知,在加密阶段,本文方案的时间开销较 dPRES 方案高。搜索阶段是统计搜索不同数量关键字的时间开销,如图 2 所示。

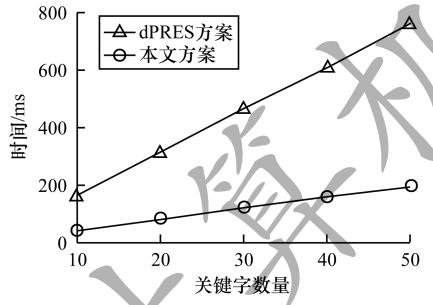

图 2 关键字数量对搜索时间的影响

Fig. 2 Effect of the number of keywords on the search time

由图 2 可知,在搜索阶段,当关键字数量为10 个时,本文方案的时间开销为 42 ms,而 dPRES 方案的时间开销为 164.4 ms;当关键字数量为30 个时,本文方案的时间开销为 122.4 ms,而 dPRES 方案的时间开销为 456.2 ms;当关键字数量为50 个时,本文方案的时间开销为 198.9 ms,而 dPRES 方案的时间开销为 762.2 ms。随着关键字数量的增加,dPRES 方案的时间开销增长速率比本文方案大,说明本文方案的搜索效率优于 dPRES 方案。

统计在不同数量关键字下的解密开销时间,如图 3 所示。

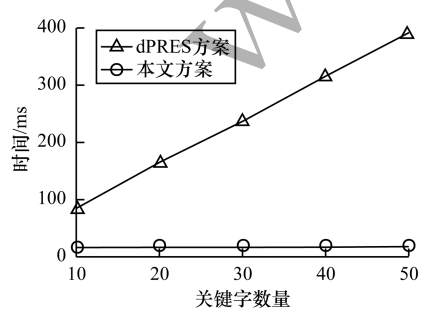

图 3 关键字数量对解密时间的影响

Fig. 3 Effect of the number of keywords on decryption time

由图 3 可以看出,在解密阶段,随着关键字数量的增大,本文方案的时间开销几乎保持不变;当关键字数量为 10 个时,dPRES 方案的时间开销为 85.7 ms;当关键字数量为 30 个时,dPRES 方案的时间开销为 236.5 ms;当关键字数量为 50 个时,dPRES 方案的时间开销为 390.8 ms,说明 dPRES 方案的时间开销与关键字数量之间呈线性增长。因此,本文方案的解密效率优于 dPRES 方案。

由图 1 ~ 图 3 可知,虽然在加密阶段,本文方案的时间开销较 dPRES 方案高,但是在搜索阶段,本文方案时间开销远远小于 dPRES 方案,且在解密阶段,本文方案时间开销也低于 dPRES 方案。因此,本文方案在解密算法和搜索算法的计算代价上有明显优势,减少了电子邮箱服务器和用户之间的通信代价,提高了系统的性能。

6 结束语

为解决密文授权和密文搜索问题,本文提出一种面向电子邮件支持高效关键字搜索的 PRE 方案。该方案在搜索过程中只用了一个双线性对,因此搜索效率较高。同时,本文方案在标准模型下关键字隐私、密文隐私和陷门隐私是安全的,还可以抵抗篡改攻击和关键字猜测攻击。分析结果表明,相对 dPRES 方案,本文方案在搜索效率上有较大的提升。目前,支持关键字搜索的 PRE 方案还有一些问题需要解决,如进一步减少时间开销,提高方案的计算效率和通信效率等,这将是下一步的研究方向。

参考文献

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography [C]// Proceedings of International Conference on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1998: 127-144.

[2] ATENIESE G, FU K, GTEEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security, 2006, 9(1): 1-30.

[3] CANETTI R, HOHENBERGER S. Chosen-ciphertext secure proxy re-encryption[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2007: 185-194.

[4] CANARD S, DEVIGNE J, LAGUILLAUMIE F. Improving the security of an efficient unidirectional proxy re-encryption scheme [J]. Journal of Internet Services and Information Security, 2011, 1(2): 140-160.

[5] CHOW S S M, WENG J, YANG Y J, et al. Efficient unidirectional proxy re-encryption[C]//Proceedings of International Conference on Cryptology in Africa. Berlin, Germany: Springer, 2010: 316-332.

[6] LIN Hanyu. Secure content distribution using multi-hop proxy re-encryption[J]. Wireless Personal Communications,2015,82(3):1449-1459.

[7] GUO L F,YAU W C. Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage[J]. Journal of Medical Systems,2015,39(2):11-11.

[8] XU Jieru, CHEN Kefei, SHEN Zhonghua, et al. Improved certificate-based conditional proxy re-encryption scheme[J]. Journal of Cryptologic Research,2018,5(4):344-358. (in Chinese)
徐洁如,陈克非,沈忠华,等. 改进的基于证书条件代理重加密方案[J]. 密码学报,2018,5(4):344-358.

[9] SU Mang, WU Bin, FU Anmin, et al. Proxy re-encryption based assured update scheme of authorization for cloud data[J/OL]. Journal of Software:1-11[2019-08-20]. http://kns.cnki.net/kcms/detail/11.2560.TP.20190122.1348.002.html(in Chinese)
苏锟,吴槟,付安民,等. 基于代理重加密的云数据访问授权确定性更新方案[J/OL]. 软件学报:1-11[2019-08-20]. http://kns.cnki.net/kcms/detail/11.2560.TP.20190122.1348.002.html

[10] JIANG Mingming,GUO Yuyan,YU Lei,et al. Efficient identity-based proxy re-encryption on lattice in the standard model[J]. Journal of Electronics & Information Technology,2019,41(1):61-66. (in Chinese)
江明明,郭宇燕,余磊,等. 有效的标准模型下格上基于身份的代理重加密[J]. 电子与信息学报,2019,41(1):61-66.

[11] SHAO Jun, CAO Zhenfu, LIANG Xiaohui, et al. Proxy re-encryption with keyword search [J]. Information Sciences,2010,180(13):2576-2587.

[12] CHEN Xi, LI Yong. Efficient proxy re-encryption with private keyword searching in untrusted storage [J]. International Journal of Computer Network and Information Security,2011,3(2):50-56.

[13] GUO Lifeng, HU Lei. Efficient bidirectional proxy re-encryption with direct chosen-ciphertext security [J]. Computers & Mathematics with Applications, 2012, 63(1):151-157.

[14] GUO Lifeng, LU Bo. Efficient proxy re-encryption with keyword search scheme [J]. Journal of Computer Research and Development,2014,51(6):1221-1228.

[15] RHEE H S, PARK J H, SUSILO W, et al. Trapdoor security in a searchable public-key encryption scheme with a designated tester [J]. Journal of Systems and Software,2010,83(5):763-771.

[16] WANG C H, TU T Y. Keyword search encryption scheme resistant against keyword-guessing attack by the untrusted server [J]. Journal of Shanghai Jiaotong University(Science),2014,19(4):440-442.

[17] LIU Zhenhua,ZHOU Peilin,DUAN Shuhong. Attribute-based proxy re-encryption scheme with keyword search[J]. Journal of Electronics & Information Technology,2018,40(3):683-689. (in Chinese)
刘振华,周佩琳,段淑红. 支持关键词搜索的属性代理重加密方案[J]. 电子与信息学报,2018,40(3):683-689.

[18] GUO Lifeng,LU Bo. Efficient proxy re-encryption with keyword search scheme [J]. Journal of Computer Research and Development, 2014, 51(6):1221-1228. (in Chinese)
郭丽峰,卢波. 有效的带关键字搜索的代理重加密方案[J]. 计算机研究与发展,2014,51(6):1221-1228.

[19] GUO Lifeng, LI Ting. Improved proxy re-encryption with keyword search scheme [J]. Journal of Shanxi University(Natural Science Edition),2016,39(3):434-441. (in Chinese)
郭丽峰,李婷. 改进的带关键字搜索的代理重加密方案[J]. 山西大学学报(自然科学版),2016,39(3):434-441.

[20] SHAO Jun, LIU Peng, CAO Zhenfu, et al. Multi-use unidirectional proxy re-encryption[C]//Proceedings of IEEE International Conference on Communications. Kyoto,Japan:[s.n.],2011:5-9.

[21] HAN Xiao, ZENG Qi, CAO Yongming. An efficient proxy re-encryption scheme with keyword search[J]. Computer and Modernization, 2019(3):117-121. (in Chinese)
韩笑,曾琦,曹永明. 一种有效的带关键字搜索的代理重加密方案[J]. 计算机与现代化,2019(3):117-121.

[22] YE Weiwei,OU Qingyu,WEI Wei. Provably secure identity-based conditional proxy re-encryption scheme[J]. Computer Engineering,2017,43(9):194-198. (in Chinese)
叶伟伟,欧庆于,魏巍. 可证安全的基于身份条件代理重加密方案[J]. 计算机工程,2017,43(9):194-198.

编辑　刘继娟