一种改进的PETKS原型方案及其扩展

崔国华 徐 鹏 雷凤宇

(华中科技大学计算机科学与技术学院信息安全实验室 武汉 430074)

摘 要 关键字可搜索的公钥加密是对基于身份加密方案的直接应用,是一种具有特殊功能和全新应用环境的方案。2005年Abdalla等人首次提出了具有临时关键字可搜索的公钥加密的原型方案。在该原型方案的基础上,研究了该方案存在的效率问题,提出了一种更高效的实例方案,并从中抽象出更高效的原型方案。在原型方案的基础上,提出了两种扩展的原型方案,从而进一步丰富了该方案的应用环境。

关键词 关键字可搜索的公钥加密,基于身份加密方案,具有临时关键字可搜索的公钥加密

Improved Prototype Scheme of PETKS and its Expansion

CUI Guo-hua XU Peng LEI Feng-yu

(Lab. of Information Security, College of Computer Science, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Public-Key Encryption with Keyword Search is an application of Identity-Based Encryption scheme, and an interesting scheme with special functions and new application. In 2005, Abdalla et al. firstly proposed a prototype scheme of Public-Key Encryption with Temporary Keyword Search, based on it, researched the efficiency of it, proposed a more efficiently instantial scheme, and extracted a more efficient prototype scheme from this instantial scheme. Based on this proposed prototype scheme, proposed two kinds of expansions, and then enriched the applications of this prototype scheme.

Keywords Public-key encryption with keyword search, Identity-based encryption scheme, Public-key encryption with temporary keyword search

1 引言

基于身份的加密方案(Identity-based Encryption scheme, IBE scheme)[1]是一类特殊的公钥加密方案,它以任意字符串作为用户的公钥进行加密,从而取消了传统PKI技术对在线密钥管理中心的需要,因此在很大程度上提高了系统效率,特别是在线密钥管理中心的性能瓶颈问题。

1984年Shamir提出了IBE的概念,但实用IBE方案直到2001年才出现。通过采用双线性映射,2001年Boneh和Franklin[2]提出了第一个实用的和随机预言机模型下可证明安全的IBE方案。随后2004年Boneh等人[3,4]基于双线性映射提出了两个标准模型下可证明安全的IBE方案,但由于它们均存在缺陷,因而实用性并不理想。2005年Waters[5]提出了第一个实用的和标准模型下可证明安全的IBE方案,它标志着IBE方案在可证明安全领域取得了基本的成功。

IBE方案在实用性和安全性取得认可的同时,基于IBE方案的应用也开始出现。2004年Boneh[6]在欧密会上首次提出了关键字可搜索的公钥加密(Public-Key Encryption with Keyword Search, PEKS)(具体含义见第2节),它是IBE方案最直接和有意义的应用。在Boneh的基础上,2005年Abdalla等人[7]对PEKS的理论部分做了完整的修正和补充,并且进一步扩展了PEKS的应用(或者功能),特别是具有临时关键字可搜索的公钥加密方案(Public-Key Encryption with Temporary Keyword Search, PETKS)和搜索结果满足布尔公式的PEKS方案。

为了实现PETKS方案,文献[7]分等级的基于身份加密体制(Hierarchical Identity-Based Encryption scheme, HIBE scheme),提出了通用的且高度形式化的原型方案,但是并没有考虑效率问题。例如在文献[7]的PETKS方案中,邮件服务器每一次验证时必须进行一次解密操作。通过研究基于IBE及HIBE方案的PETKS方案的特点后,本文提出了一个更高效的基于IBE方案的PETKS方案实例,该方案中邮件服务器只在满足特定条件时才需要进行解密操作并完成验证,而其它时候只需进行一次简单的判断即可完成验证过程。本文在改进后的PETKS方案的基础上抽象出基于IBE方案的PETKS原型方案。此外,基于提出的PETKS原型方案提出了两种扩展方案,从而进一步丰富了该类PETKS原型方案的应用。

有关PEKS和PETKS方案的介绍将在下一节给出。

2 预备知识

2.1 IBE方案

到稿日期:2008-04-16 本文受国家自然科学基金项目(编号:60703048),湖北省自然科学基金项目(编号:2007ABA313)资助。

崔国华 博士生导师,教授,研究方向为现代密码学、网络安全及算法分析等;徐 鹏 博士生,研究方向为现代密码学、网络安全等,E-mail:xupeng0328@hotmail.com;雷凤宇 博士生,研究方向为传感器网络、公钥密码等。

IBE方案由4个算法组成，分别是系统的初始化算法Setup、用户公私钥生成算法Extract、加密算法Encrypt、解密算法Decrypt。由于本文将基于BF方案(由Boneh和Franklin[2]提出的第一个实用的和RO模型下可证明安全的IBE方案的简称)构建PETKS方案实例，因此本节将简要介绍该IBE方案。

具有IND-ID-CPA安全性[2]和匿名性[6]的BF方案由以下4个算法组成：

1) $Setup(k)$：给定安全参数 $k\in Z^*$，生成系统参数 $params=\langle q,G_1,G_2,\hat{e},n,P,P_{pub},H_1,H_2\rangle$ 和主密钥 $s\in Z_q^*$，其中 G_1,G_2 为大素数 q 阶群，$\hat{e}:G_1\times G_1\rightarrow G_2$，$n$ 为明文空间的长度，P 为 G_1 的生成元，$P_{pub}=sP$，$H_1:\{0,1\}^*\rightarrow G_1^*$，$H_2:G_2\rightarrow\{0,1\}^n$。

2) $Extract(ID)$：给定用户 $ID\in\{0,1\}^*$，该用户的公钥为 $Q_{ID}=H_1(ID)$，私钥为 $d_{ID}=sQ_{ID}$。

3) $Encrypt(ID,m)$：给定用户身份ID和明文 m，计算该用户公钥 $Q_{ID}=H_1(ID)$；选择随机数 $r\in Z_q^*$，则密文 $C=\langle rP,H_2(\hat{e}(Q_{ID},P_{pub})^r)\oplus m\rangle$。

4) $Decrypt(C,d_{ID})$：令 $C=\langle U,V\rangle$。用户ID的私钥为 d_{ID}，则解密 C，使得明文 $m=V\oplus H_2(\hat{e}(d_{ID},U))$。

2.2 PEKS与PETKS方案

本节首先以一个重要的应用实例来说明PEKS方案的设计目的和作用。以邮件系统为例，接收者希望建立一个邮件路由系统，能够接收所有加密发送给它的邮件，并且能够按照邮件所含关键字将邮件分发到接收者拥有的和不同的接收器上，从而使得接收者可以按不同的优先级处理邮件，并且整个处理过程中邮件路由系统均无法知道关键字的内容。由此可以总结出，PEKS方案可以实现公钥加密信息的分类和检索，并且除接收者外分类和检索信息不会被泄露。

为了方便后文对PEKS应用的扩展，本文将PEKS的应用归结到一个最直接和最基本的功能上，即邮件服务器按照接收者的要求返回含有特定关键字的邮件。除了功能方面的要求外，PEKS方案在安全性上要求邮件路由系统只能判断该邮件是否含有特定关键字，但并不知道该关键字的内容。

定义2.1 一个PEKS方案由以下4个概率多项式时间算法组成：

1) $KeyGen(s)$：输入安全参数 s，生成公私钥对 A_{pub},A_{priv}。

2) $PEKS(A_{pub},W)$：输入公钥 A_{pub} 和关键字 W，生成关于 W 的可搜索加密。

3) $Trapdoor(A_{priv},W)$：输入私钥 A_{priv} 和关键字 W，生成陷门信息 T_W。

4) $Test(A_{pub},S,T_W)$：输入公钥 A_{pub}、可搜索加密 $S=PEKS(A_{pub},W')$ 和陷门信息 $T_W=Trapdoor(A_{priv},W)$，若 $W=W'$，则输出"1"，否则输出"0"。

以上4个算法的具体使用过程如下：

1)发送者 B 利用算法 $PEKS()$ 生成含有关键字可搜索的和公钥加密的邮件信息，即 $[E_{A_{pub}}[msg],PEKS(A_{pub},W_1),\cdots,PEKS(A_{pub},W_k)]$，其中 E 为某公钥加密算法，A_{pub} 为接收者的公钥。并将该邮件发送给邮件服务器。

2)接收者 A 利用算法 $Trapdoor()$ 生成关键字 W 的陷门信息 T_W，并发送给邮件服务器。

3)邮件服务器利用算法 $Test()$ 验证并找出那些邮件含有与陷门信息 T_W 一致的关键字，并将该邮件返回给接收者。

以上即为PEKS基本的应用及其实现思想。从上述可以看出，邮件服务器一旦拥有了关键字 W 的陷门信息 T_W，则可以一直验证某邮件是否含有该关键字，因此为了限制邮件服务器的验证能力只在某时间有效，扩展了PEKS的应用，并称可验证性受时间约束的PEKS方案为具有临时关键字可搜索的公钥加密方案，即PETKS方案。

3 改进的PETKS方案

本节基于BF方案首先提出一个PETKS方案实例(简称为PETKS-I方案)，并在此基础上抽象出基于IBE方案的PETKS原型方案(简称为PETKS-P原型方案)。

PETKS-I方案由以下4个算法组成：

1) $KeyGen(s)$：运行BF方案的系统初始化算法 $Setup(s)$，生成主密钥 $s\in Z_q^*$ 和系统参数 $params=\langle q,G_1,G_2,\hat{e},n,P,P_{pub},H_1,H_2\rangle$(其含义参考2.1节)。

2) $PEKS(params,W,t)$：输入系统参数 $params$，关键字 W，时间 t，运行BF方案的公私钥生成算法 $Extract(W||t)$ 生成 t 时刻 W 的公钥 $Q_W=H_1(W||t)$；选取随机值 $R\in\{0,1\}^n$，运行BF方案的加密算法 $Encrypt(W||t,R)$，生成可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W,R)\rangle$(显然可以看出，PETKS-I方案以关键字和时间信息的联接替代BF方案中的身份信息，并生成相应的公钥进行加密。由于IBE方案并不对身份信息有任何特殊的要求，因此该算法的执行并不会产生兼容性问题。)

3) $Trapdoor(s,W,t')$：输入主密钥 s、关键字 W 和时间 t'，运行BF方案的公私钥生成算法 $Extract(W||t')$，先生成公钥 $Q_W'=H_1(W||t')$，再生成对应的私钥 $d_W'=sQ_W'$，输出 $\langle d_W',t'\rangle$。

4) $Test(params,S,\langle d_W',t'\rangle)$：输入系统参数 $params$、可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W,R)\rangle$ 和私钥 $\langle d_W',t'\rangle=Trapdoor(s,W,t')$；按位取 S 中的时间 t，若 $t'=t$ 则继续，否则输出"0"；运行BF方案的解密算法 $R'=Decrypt(Encrypt(Q_W,R),d_W')$，按位取 S 中的 R，若 $R=R'$ 则输出"1"，否则输出"0"。

以上即为完整的PETKS-I方案描述。根据以上算法可以看出，由于邮件服务器能否验证可搜索加密，完全取决于它是否具有由指定的时间和关键字生成的私钥，因此即使同一关键字在不同时刻生成的可搜索加密，由于它们两个的私钥不可能相同(除了一个可忽略的碰撞概率)，故不能用于验证对方的可搜索加密。从另一个方面说，接收方可以通过只传递给邮件服务器指定时间和关键字的私钥，使得其只具有验证该时刻生成的具有相同关键字的可搜索加密，从而实现了可验证性受时间约束的公钥加密方案，即实现了PETKS方案。

在上述算法中，对文献[7]最重要的一点改进是可搜索加密 $S=\langle R||t,Encrypt(Q_W,R)\rangle$ 中的 $R||t$ 和 $\langle d_W',t'\rangle=Trapdoor(s,W,t')$。在文献[7]中邮件服务器的每一次验证必须运行一次解密运算，而在PETKS-I方案中只有当 $t'=t$ 时才进行解密操作，即由时间参数作为条件在运行解密操作前即将一部分不满足条件的可搜索加密淘汰，由于判断等式 $t'=t$ 是否成立的时间远小于解密运算，因此PETKS-I方案

明显具有更高的效率。

虽然 PETKS-I 方案与文献[7]存在差别，但并不影响其安全性。由于关键字 W 和时间 t 的联接等价于身份信息，因此时间 t 的泄露并不会影响 BF 方案的安全性(IBE 方案中身份信息是公开的)。又因为基于 IBE 方案构建的 PETKS 方案的安全性依赖于该 IBE 方案的安全性[7]，所以 BF 方案的安全性不受影响，则 PETKS-I 方案依然安全。

在 PETKS-I 方案的基础上，本文将抽象出基于 IBE 方案的 PETKS 原型方案，从而给出该类 PETKS 方案的通用构造方法。PETKS-P 原型方案由以下 4 个算法构成：

1) $KeyGen(s)$：运行 IBE 方案的系统初始化算法 $Setup(s)$，生成主密钥 s 和系统参数 $params$。

2) $PEKS(params,W,t)$：输入系统参数 $params$、关键字 W 和时间 t，运行 IBE 方案的公私钥生成算法 $Extract(W||t)$，生成 t 时刻 W 的公钥 Q_W^t；选取随机值 $R\in\{0,1\}^n$，运行 IBE 方案的加密算法 $Encrypt(W||t,R)$，生成可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W^t,R)\rangle$。

3) $Trapdoor(s,W,t')$：输入主密钥 s、关键字 W 和时间 t'，运行 IBE 方案的公私钥生成算法 $Extract(W||t')$，先生成私钥 $d_W^{t'}$，输出$\langle d_W^{t'},t'\rangle$。

4) $Test(params,S,\langle d_W^{t'},t'\rangle)$：输入系统参数 $params$、可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W^t,R)\rangle$ 和私钥$\langle d_W^{t'},t'\rangle=Trapdoor(s,W,t')$，按位取 S 中的时间 t，若 $t'=t$ 则继续，否则输出“0”；运行 IBE 方案的解密算法 $R'=Decrypt(Encrypt(Q_W^t,R),d_W^{t'})$，按位取 S 中的 R，若 $R=R'$则输出“1”，否则输出“0”。

以上即为完整的 PETKS-P 原型方案的描述。虽然该原型方案并不依赖于具体的 IBE 方案，但是由于该类 PETKS 方案的安全性依赖于具体的 IBE 方案，因此通过具体的 IBE 方案构建 PETKS 方案时要求该 IBE 方案必须满足特定的安全性(具体内容参考文献[7])。

4 基于 PETKS-P 原型方案的扩展

作为一种全新的和具有特殊功能的方案，PETKS 方案的扩展显得尤为重要，它不仅可以开拓该方案的应用领域，甚至有可能解决目前存在的一些应用难题。

通过对上一节 PETKS-P 原型方案的研究和扩展，本节提出两种扩展后的原型方案，并且分别实现：可验证性在接收方提出的时间区间内有效的 PETKS 原型方案(简称为 RT$[t_i,t_j]$-PETKS-P 原型方案，其中 $t_i<t_j$)和可验证性在发送方提出的时间区间内有效的 PETKS 原型方案(简称为 ST$[t_i,t_j]$-PETKS-P 原型方案)。

4.1 RT$[t_i,t_j]$-PETKS-P 原型方案

RT$[t_i,t_j]$-PETKS-P 原型方案是指邮件服务器的可验证性在接收者的指定时间区间内有效。为此，接收方需要为指定的关键字和指定的时间区间内每一个时间点生成验证用的私钥。具体的方案由以下 4 个算法组成：

1) $KeyGen(s)$：运行 IBE 方案的系统初始化算法 $Setup(s)$，生成主密钥 s 和系统参数 $params$。

2) $PEKS(params,W,t)$：输入系统参数 $params$、关键字 W 和时间 t，运行 IBE 方案的公私钥生成算法 $Extract(W||t)$，生成 t 时刻 W 的公钥 Q_W^t；选取随机值 $R\in\{0,1\}^n$，运行 IBE 方案的加密算法 $Encrypt(W||t,R)$，生成可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W^t,R)\rangle$。

3) $Trapdoor(s,W,[t_i,t_j])$：输入主密钥 s、关键字 W 和时间区间$[t_i,t_j]$，为时间区间$[t_i,t_j]$内的每一个时间点 $t_k\in[t_i,t_j]$运行 IBE 方案的公私钥生成算法 $Extract(W||t_k)$，先生成私钥$\langle d_W^{t_k},t_k\rangle$，输出所有的私钥 $d_W^{[t_i,t_j]}=\{\langle d_W^{t_i},t_i\rangle,\cdots,\langle d_W^{t_k},t_k\rangle,\cdots,\langle d_W^{t_j},t_j\rangle\}$。

4) $Test(params,S,d_W^{[t_i,t_j]})$：输入系统参数 $params$、可验证性受时间约束的可搜索加密 $S=\langle R||t,Encrypt(Q_W^t,R)\rangle$ 和私钥集 $d_W^{[t_i,t_j]}=Trapdoor(s,W,[t_i,t_j])$；对每一个私钥$\langle d_W^{t_k},t_k\rangle\in d_W^{[t_i,t_j]}$ 进行如下处理：

(1) 按位取 S 中的时间 t，若 $t_k=t$ 则继续，否则输出“0”；

(2) 运行 IBE 方案的解密算法 $R'=Decrypt(Encrypt(Q_W^t,R),d_W^{t_k})$，按位取 S 中的 R，若 $R=R'$则输出“1”，否则输出“0”。

以上即为完整的 RT$[t_i,t_j]$-PETKS-P 原型方案的描述。由于邮件服务器只具有指定关键字在特定时间区间内的私钥，因此它不可能验证该时间区间外的具有相同关键字的可搜索加密。

由于 PETKS-P 原型方案的效率比文献[7]中的同类方案有明显的提高，因此 RT$[t_i,t_j]$-PETKS-P 原型方案的效率比文献[7]中的同类扩展方案依然有明显的提高。

4.2 ST$[t_i,t_j]$-PETKS-P 原型方案

ST$[t_i,t_j]$-PETKS-P 原型方案是指邮件服务器的可验证性在发送者的指定时间区间内有效。为此，发送方需要为指定的关键字和指定的时间区间内每一个时间点生成可搜索加密。具体的方案由以下 4 个算法组成：

1) $KeyGen(s)$：运行 IBE 方案的系统初始化算法 $Setup(s)$，生成主密钥 s 和系统参数 $params$。

2) $PEKS(params,W,[t_i,t_j])$：输入系统参数 $params$、关键字 W 和时间区间$[t_i,t_j]$；对每一个时间点 $t_k\in[t_i,t_j]$做如下处理：

(1) 运行 IBE 方案的公私钥生成算法 $Extract(W||t_k)$，生成 t_k 时刻 W 的公钥 $Q_W^{t_k}$；

(2) 选取随机值 $R\in\{0,1\}^n$，运行 IBE 方案的加密算法 $Encrypt(W||t_k,R)$，生成可验证性受时间约束的可搜索加密 $S_k=\langle R||t_k,Encrypt(Q_W^{t_k},R)\rangle$。

最后输出所有时间点的可搜索加密，即 $S(W,[t_i,t_j])=\{S_i=\langle R||t_i,Encrypt(Q_W^{t_i},R)\rangle,\cdots,S_k=\langle R||t_k,Encrypt(Q_W^{t_k},R)\rangle,\cdots,S_j=\langle R||t_j,Encrypt(Q_W^{t_j},R)\rangle\}$。

3) $Trapdoor(s,W,t')$：输入主密钥 s、关键字 W 和时间 t'，运行 IBE 方案的公私钥生成算法 $Extract(W||t')$，先生成私钥 $d_W^{t'}$，输出$\langle d_W^{t'},t'\rangle$。

4) $Test(params,S(W,[t_i,t_j]),\langle d_W^{t'},t'\rangle)$：输入系统参数 $params$、可验证性受时间约束的可搜索加密集 S 和私钥$\langle d_W^{t'},t'\rangle$；对每一个可搜索加密 $S_k\in S$ 做如下处理：

(1) 按位取 S_k 中的时间 t_k，若 $t'=t_k$ 则继续，否则输出“0”；

(2) 运行 IBE 方案的解密算法 $R'=Decrypt(Encrypt(Q_W^{t_k},R),d_W^{t'})$，按位取 S_k 中的 R，若 $R=R'$则输出“1”，否则

(下转第 64 页)

结束语 本文提出了一种分层环形 NoC 拓扑结构，该结构中链路分为两组环网，其中有一组环网为备用环网，用于系统的容错机制。设计了一种时分和空分复用的路由算法、分离控制和数据，去除了数据缓存，消除了链路拥塞，较好地解决了当前 NoC 研究中的几个关键问题。目前正在采用 FPGA 对该结构进行验证，并把该结构用于 TD-SCDMA 的基站的各个单元的通信。

参 考 文 献

[1] Dally W, Towles B. Route packets, not wires: on-chip interconnection networks // Proc. the Design Automation Conference. Las Vegas, NV, 2001: 684-689

[2] Hemani A, Jantsch A, Kumar S, et al. Network on a chip: an architecture for billion transistor era // Proc. IEEE NorChip Conference. 2000: 166-173

[3] Ye T. On-chip multiprocessor communication network design and analysis. PhD Dissertation. Stanford University, 2003

[4] Hu J, Marculescu R. Energy- and performance-aware mapping for regular NoC architectures. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, 2005, 24(4): 551-562

[5] Goossens K. Formal methods for networks on chips // Proc. Fifth International Conference on Application of Concurrency to System Design. 2005: 188-189

[6] Hansson A, Goossens K, Rădulescu A. A unified approach to constrained mapping and routing on network-on-chip architectures // Proceedings of the 3rd IEEE/ACM/IFIP international …. 2005

[7] Pirretti M, Link G M, Brooks R R. Fault tolerant algorithms for network-on-chip interconnect // VLSI, 2004. Proceedings. IEEE Computer Society Annual …. 2004

[8] Bolotin E, Cidon I, Ginosar R, et al. QNoC: QoS architecture and design process for network on chip. Journal of Systems Architecture, 2004

[9] Banerjee N, Vellanki P, Chatha K S. A Power and Performance Model for Network-on-Chip Architectures // Proceedings of DATE. 2004

[10] Jantsch A. The Nostrum Network on Chip. Stockholm: Royal Institute of Technology, 2003

[11] Urbansky R. Transmission system for the synchronous digital hierarchy. US Patent 5,343,476, 1994

[12] Davik F, Yilmaz M, Gjessing S, et al. IEEE 802. 17 resilient packet ring tutorial. Communications Magazine, IEEE, 2004

[13] Siguenza-Tortosa D, Nurmi J. Sigüenza-Tortosa D, et al. Proteo: A New Approach to Network-on-Chip // Proceedings of the IASTED International Conference on Communication Systems and Networks. 2002: 355-357

[14] Samuelsson H, Kumar S. Ring Road Network on Chip Architecture // Proceedings, Norchip Conference. 2004

[15] Guerrier P, Greiner A. A generic architecture for on-chip packet-switched interconnections // Proceedings of DATE 2000. Paris, France, March 2000

[16] Millberg M, Nilsson E, Mid R, et al. Tiuaranteed bandwidth using looped containers in temporally disjoint networks within the nostrum network on chip // Proceedings of DATE'. Paris, feb. 2004

[17] Dally W J, Towles B. Route Packets, Not Wires: On-Chip Interconnection Networks // Design Automation Conference. 2001

(上接第 60 页)

输出“0”。

以上即为完整的 ST$[t_i, t_j]$-PETKS-P 原型方案的描述。由于发送方仅生成了指定关键字在特定时间区间内的可搜索加密，因此邮件服务器对该关键字的验证只可能在该时间区间内有效(其最终的可验证性还受接收方影响)。

ST$[t_i, t_j]$-PETKS-P 原型方案为一类新的应用提供了解决办法，即有效关键字可变的加密邮件。与很多具有可变优先级的计算机体制相类似(例如进程优先级的变化等等)，通过 ST$[t_i, t_j]$-PETKS-P 原型方案可以实现。在邮件服务器中，若邮件等待的时间越长，则该邮件下一次被接收者查看的可能性更高(即具有查看频率更高的关键字)。举例说明如下：

假设关键字 W_1，W_2 的优先级为 $W_1 < W_2$(优先级越高，接收者查看的频率越高)。发送方采用 ST$[t_i, t_j]$-PETKS-P 原型方案生成可搜索加密 $S(W_1, [t_i, t_j])$ 和 $S(W_2, [t'_i, t'_j])$，其中 $t_j < t'_i$，且令邮件为$[E_{A_{pub}}[msg], S(W_1, [t_i, t_j]), S(W_2, [t'_i, t'_j])]$。显然可以看出，时间$[t_i, t_j]$内由于仅有关键字 W_1 有效，因此该邮件具有较低的优先级。类似地，时间$[t'_i, t'_j]$内关键字 W_2 生效而关键字 W_1 无效，因此该邮件在时间$[t'_i, t'_j]$内具有较高的优先级，从而该邮件在时间$[t'_i, t'_j]$内被接收者查看的可能性增大，即实现了有效关键字可变的加密邮件。

结束语 根据文献[7]提出的 PETKS 原型方案研究了该方案存在的效率问题，即邮件服务器每一次验证都必须进行一次解密操作。本文提出了改进后的方案实例，并在此基础上提出了基于 IBE 方案的 PETKS 原型方案，从而使得该类原型方案的效率有明显的提高。

另外，本文基于 PETKS 原型方案，提出了两种扩展的原型方案，进一步丰富了 PETKS 的应用。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C] // Advances in Cryptology-Proceedings of CRYPTO'84, LNCS. Vol. 196, Springer-Verlag, 1985: 48-53

[2] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C] // Advances in Cryptology-crypto 2001, LNCS. Vol. 2139, Springer-Verlag, 2001: 231-229

[3] Boneh D, Boyen X. Efficient Selective-ID Identity Based Encryption Without Random Oracles [C] // Advances in Cryptology-EUROENCRYPT' 2004, LNCS. Vol. 3027, Springer-Verlag, 2004: 223-238

[4] Boneh D, Boyen X. Secure Identity - based Encryption Without Random Oracles [C] // Advances in Cryptology-crypto 2004, LNCS. Vol. 3152, Springer-verlag, 2004: 443-459

[5] Waters B. Efficient Identity-based Encryption Without Random Oracles[C] // Advances in Cryptology-EUROENCRYPT'2005, LNCS. Vol. 3494, Springer-Verlag, 2005: 114-127

[6] Boneh D, Crescenzo G D, Ostrovsky R, et al. Public Key Encryption with Keyword Search [C] // Advances in Cryptology-EUROENCRYPT'2004, LNCS. Vol. 3027, Springer-Verlag, 2004: 506-522

[7] Abdalla M, Bellare M, Catalano D, et al. Searchable Encryption Revisited: Consistency Properties, Realtion to Anonymous IBE, and Extensions [C] // Advances in Cryptology-Crypto 2005, LNCS. Vol. 321, Springer-Verlag, 2005: 205-222