西安交通大學

硕士学位论文

基于 IBF 的对称可搜索加密研究与实现

学位申请人：王鹤宇

指导教师：侯迪 教授

学科名称：计算机科学与技术

XXXX 年 X 月

Research And Implementation of Symmetric Searchable Encryption Based on IBF

A thesis submitted to

Xi'an Jiaotong University

in partial fulfillment of the requirements

for the degree of

Master of Engineering

By

Heyu Wang

Supervisor: Prof. Di Hou (导师姓名全拼，例如 Anxue Zhang)

Associate Supervisor: Prof. Yong Qi

Computer Science and Technology

XXX XXXX (英文日期，月在前，年在后，例如：September 2017)

硕士学位论文答辩委员会

基于 IBF 的对称可搜索加密研究与实现

答辩人：王鹤宇

答辩委员会委员：

XXXXXXXX 大学 XXX：_____ (主席)

XXXXXXXX 大学 XXX：_____

XXXXXXXX 大学 XXX：_____

XXXXXXXX 大学 XXX：_____

XXXXXXXX 大学 XXX：_____

答辩时间：XXXX 年 XX 月 XX 日

答辩地点：XXXXXXXXXXXXXX

摘 要

随着云计算和大数据的发展，越来越多的用户数据被存放在云端。这些数据中通常包含一些敏感数据，如个人身份证号，健康记录等等。如果数据以明文形式存放在云端，则很容易导致隐私信息的泄露。因此为了保护用户的隐私数据，会在将数据上传到云服务器之前对其进行加密。为了使用云端的密文数据，通常会先用大量的网络带宽将密文下载，在本地完全解密后再检索。然而这种方案有以下两个致命缺点：1. 如果云服务器上含有大量数据，一一下载会占用大量网络带宽。2. 对已下载的文件完全解密会占用大量本地计算资源，效率极低。解决此类问题的技术称为可搜索加密 (Searchable Encryption,SE), 该技术要求只有被授权的用户才具有检索能力。

本文提出并实现了一种新的对称可搜索加密方案，并将其和已有的方案在实验上进行了对比。同数据库使用索引提高搜索效率一样，对称可搜索加密方案通常会针对明文文件集构建相应的安全索引 (不泄露相应明文文件集合信息的索引)。本文基于一种新型的数据结构——不可区分布隆过滤器 (Indistinguishable Bloom Filter,IBF1)[1]，提出了一种新的安全索引构建算法。关键词在被送往云服务器进行搜索前，需要通过某种变换来隐藏关键词中的明文信息，同时使得变换后的词又能够在安全索引上进行匹配搜索。这种变换被称为陷门 (trapdoor) 生成算法，本文也提出了相应的陷门生成算法和陷门在安全索引上的搜索算法。为了验证方案的有效性，分别用 C 语言实现了我们提出的方案以及另一种基于 IBF 的可搜索加密方案。从 1. 安全索引构建时间，2. 安全索引占用的磁盘空间，3. 搜索安全索引花费的时间这三个方面对两种方案进行了对比。在真实数据集上的实验结果表明，本文提出的方案极大的减少了安全索引的构建时间和对磁盘的使用空间情况，同时搜索时间和另一方案处于同一数量级 (ms 量级)。同时本文提出的方案也满足目前提出的最强的安全模型——自适应安全模型。

安全索引占据的磁盘空间以及搜索时间 3 个方面进行了对比。本文第一次提出了使用作为树节点来构造一棵变长不可区分布隆过滤器树 (Variable-length Indistinguishable Bloomfilter Tree,VBTree) 的方式来构建安全索引，同时也给出了与 VBTree 相对应的陷门 (trapdoor) 算法以及针对相应陷门的服务器端的搜索算法。

关 键 词：对称可搜索加密，IBF，VIBtree

论文类型：应用基础

ABSTRACT

英文摘要正文每段开头不缩进，每段之间空一行。

The abstract goes here.

LaTeX is a typesetting system that is very suitable for producing scientific and mathematical documents of high typographical quality.

KEY WORDS: Xi'an Jiaotong University, Doctoral dissertation, LaTeX template

TYPE OF DISSERTATION: Application Fundamentals

目 录

CONTENTS

1 绪论

本章在第一部分介绍了可搜索加密的研究背景及意义, 在第二部分对对称可搜索加密的国内外研究现状进行了阐述，在第三部分介绍了本文的工作及贡献，在第四部分罗列出了本文的组织结构。

1.1 研究背景及意义

随着云计算和大数据的发展，越来越多的用户数据被存放在云端。这些数据中通常包含一些敏感数据，如个人身份证号，健康记录等等。如果数据以明文形式存放在云端，则很容易导致隐私信息的泄露。比如, 2013 年亚马逊的云平台受到黑客攻击, 导致 2 亿 5 千 9 百万条注册会员的个人信息被泄露。2017 年和美国某党派合作的数据分析商 Deep Root Analytics 以及 Data Trust 放在亚马逊的 1.1 TB 的数据发生泄露。因此为了保护用户的隐私数据，会在将数据上传到云服务器之前以某种加密方式对其进行加密。按照传统方式，为了使用云端的密文数据，通常会先用大量的网络带宽将密文下载，在本地完全解密后再搜索。然而这种方案有以下两个致命缺点：(1) 如果云服务器上含有大量数据，一一下载会占用大量网络带宽。(2) 对已下载的文件完全解密会占用大量本地计算资源，效率极低。解决此类问题的技术称为可搜索加密 (Searchable Encryption,SE), 在该技术中, 数据用户对感兴趣的关键词进行加密后产生陷门, 云服务器利用陷门搜索和关键词相关的数据。在可搜索加密方案中，安全性和搜索效率是最为关注的两个问题。方案满足的安全模型越强，抵抗攻击的能力就越强，用户数据泄露的可能性就越低。搜索效率越高，用户的等待时间就越短，用户体验就越好。因此，设计出高效且满足强安全模型的可搜索加密方案具有非常重要的意义。

1.2 国内外研究现状

可搜索加密技术分为两大类：对称可搜索加密 (Symmetric Searchable Encryption, SSE) 和非对称可搜索加密 (Asymmetric Searchable Encryption, ASE)。非对称可搜索加密又被称作公钥可搜索加密 (Public key Encryption with Keyword Search, PEKS)。两类技术在构造方法和使用场景方面都有不同, 具体来讲:(1) 两类技术的构造方法不同。其中,SSE 方案的构造基于对称密码原语来设计。一般有两方参与者: 数据拥有者和云服务器。数据拥有者用私钥加密数据后外包给云服务器, 之后数据拥有者使用私钥搜索云服务器中的数据。与之对应的 PEKS 方案的构造基于公钥密码原语。一般有三方参与者: 数据拥有者、云服务器和用户。数据拥有者用公钥加密数据后外包给云服务器, 之后用户使用私钥搜索云服务器中的数据。由于 PEKS 方案基于公钥密码构造, 因此方案的构造效率低下。(2) 两类方法的应用场景不同。SSE 的应用场景多样, 如财务数据、医疗数据、政府数据等私有数据库的外包与搜索, 与之对应的 PEKS 主要应用于加密邮件系统。基于上述两个原因,SSE 技术成为近年来学术界的研究热点, 大量 SSE 方案被提出。

目前, SSE 方案的研究内容主要分为如下四个方面: (1) 单关键词搜索: 单关键词搜索是 SSE 的基本搜索方式, 即返回包含单个搜索关键词的所有文档。在单关键词搜索方面, 如何提高搜索效率和安全性成为研究热点; (2) 多模式搜索: 为了构造更加实用的 SSE 方案, 需要支持更加丰富搜索的方式, 如多关键词搜索、模糊关键词搜索、搜索结果排序和范围查询等; (3) 前/后向安全搜索: 动态 SSE 方案需要支持文件的更新和删除, 但是在动态更新中会泄漏重要信息, 如何保证动态 SSE 方案的前/后向安全成为关键; (4) 可验证搜索: 在恶意服务器模型中, 如何设计可验证的 SSE 方案, 即验证服务器返回结果的正确性和完整性成为必要。接下来主要从这 4 个方面对 SSE 的研究现状进行阐述。

1.2.1 单关键词搜索

2000 年，Song[2] 等人首次提出了不可信赖服务器的存储问题，同时提出了第一个基于密文扫描思想的对称可搜索加密方案。其方案在加密时将明文文件划分为“单词”，然后对其分别加密，搜索时通过对整个密文文件和密文单词进行比对，就可确认关键词是否存在，甚至统计其出现的次数。其缺点也很明显，首先必须使用固定大小的“单词”，即通常要对文中的单词进行填充到固定长度变为“单词”，此外，搜索时搜索效率较低，需要对密文进行全文扫描。2003 年，Goh[3] 等人首次提出了安全索引的概念，并提出了第一个安全模型——针对选择关键词攻击下的语义安全 (semantic security against adaptive chosen keyword attack, IND-CKA), 并且也给出了一个基于布隆过滤器[4](Bloom Filter, BF) 且满足 IND-CKA 安全模型的 Z-IDX 方案。其方案使用布隆过滤器作为单个文件的索引结构, 将文件包含的关键词映射为码字存储于该文件的索引中, 通过布隆过滤器的运算, 就能判定密文文件是否包含某个特定关键词，较全文扫描思想方案而言极大的提升了搜索效率。其缺点来源于布隆过滤器中存在的误判问题。2005 年，Chang[5] 等人考虑了可搜索加密基本问题的一个应用场景: 用户通过个人电脑将明文文件加密后存放至云服务器, 然后使用移动设备 (例如手机等) 搜索服务器上的密文文件, 并针对此问题了提出了 PPSED(privacy preserving keyword searches on remoted encrypted data) 方案。其方案利用关键词字典集合给文件建立索引, 索引的大小和关键词字典的数量相同。该方案可以实现对文件的精确搜索, 解决了布隆过滤器方案当中存在的误判问题。2006 年，Curtmola[6] 等人规范化了对称可搜索加密及其安全目标, 同时提出了能在非自适应和自适应安全模型下达到不可区分性安全的 SSE-1 和 SSE-2 方案。类似于倒排索引的构建方式，SSE-1 和 SSE-2 都是基于“关键词-文件”索引构建思想, 服务器只需 O(1) 时间即可完成搜索操作。然而, 执行文件的添加或删除操作需要重新构建索引, 时间开销较大。

1.2.2 多模式搜索

仅仅使用单关键词搜索会使得服务器返回大量满足搜索条件的文档, 为了进一步筛选出想要的文档, 支持多模式的 SSE 方案引起人们的关注，比如连接关键词搜索 (同时搜索多个关键词)、模糊关键词搜索 (同时搜索输入关键词的同义词)、排序搜索 (对查询

结果进行排序，返回 top-K 的结果) 和范围查询 (对数值型数据的区间查询，如年龄位于 18 岁以上的) 等。接下来四段分别回顾了这几种模式的研究进展。

2004 年，Golle[7] 等人第一次提出了 2 个支持多个连接关键词搜索的方案 GSW-1 和 GSW-2。GSW-1 方案的缺点是关键词的陷门大小与加密文档的数量成线性关系，GSW-2 方案利用双线性映射实现了常量大小的关键词陷门，但是判断一个文档需要计算两次双线性对。2005 年，Ballard[8] 等人也构造了两个基于连接关键词的可搜索加密方案 SCKS-SS 和 SCKS-XDH，其缺点和 Golle 等人提出的方案相同，都有大量的模指数运算和双线对运算，并且搜索复杂度都与文档数量线性相关。因此, 其搜索效率不高。Byun [9] 等人和 Ryu [10] 等人分别利用双线性对构造了基于连接关键词的可搜索加密方案 BLL 和 RT，方案的特点都是关键词陷门大小固定，但是判断每个文档都需要计算两次双线性对。2013 年，Cash[11] 等人提出了首个亚线性的连接关键词查询方案 (Oblivious Cross-Tags, OXT)。其方案主要思想分为两步：首先, 选取频率最小的关键词 (在所有搜索的关键词中, 频率最小的关键词对应的文档数最少) 来搜索; 然后, 判断搜索结果是否包含其它搜索的关键词, 若该结果包含其它所有的搜索关键词, 则该结果是最终的搜索结果。Lai[12] 等人指出 Cash 的方案存在结果模式泄露问题：即对于每个文档，知道其是否包含除了最小频率关键词外的其他所有关键词的信息。为了避免这种不必要的泄露，他们提出了向量隐藏加密技术 (Hidden Vector Encryption,HVE), 并基于该技术提出结果模式隐藏的连接关键词搜索方案 HXT。传统的 SSE 方案只允许数据拥有者自身去执行搜索，为了支持多用户场景，Sun[13] 等人基于 OXT 提出了无交互的细粒度多用户 SSE 方案。在 Sun 等人提出的方案中, 不同的授权用户拥有不同的搜索和解密权限: 搜索权限为每个用户被授予不同的搜索关键词集合, 用户只能搜索被授权的关键词; 解密权限为文档标识由属性基 (Attribute-Based Encryption,ABE) 加密, 只有用户的属性满足加密策略时, 才可以解密文档标识。Wang[14] 等人指出该多用户搜索方案有严重的通信和计算代价。主要原因为: 文档标识由 ABE 加密, 服务器无法判断用户是否能解密某个加密文档。因此, 服务器需要返回所有满足搜索条件的结果, 用户需自行判断能否解密, 带来了额外的通信和解密代价。为此,Wang 等人提出了服务器端匹配的匿名属性 ABE 技术, 在不泄漏用户属性的情况下, 服务器可以判断用户能否解密密文。用此技术加密文档标识, 服务器可以仅仅返回满足搜索条件且用户能够解密的结果, 降低了通信代价并提高了解密效率。2017 年，Kamara[15] 等人指出 OXT 在执行析取关键字搜索 (返回包含任意查询关键词的文档) 时效率低下的问题, 并在 OXT 的基础上实现高效的析取关键字搜索。

2010 年，Li[16] 等人首次提出了模糊关键词检索的方案。该方案中, 采用编辑距离来定义和度量关键词间的相似度, 并使用了基于通配符和基于克 (gram) 的两种模糊关键词集构造方法。关键词查询时, 用户计算待查询关键词在编辑距离门限下的模糊陷门集合并交给服务器, 服务器使用陷门集与存储的模糊关键词集进行一一匹配, 返回可能包含被查询关键词的密文文件集合。2011 年，Brinkman[17] 等人提出包含通配符的关键词检索方法, 类似于 Z-IDX[3], 也将文件包含的关键词插入布隆过滤器. 所

不同的是, 为避免关联攻击, 该方法产生基于文件标识符的伪随机数, 用以对布隆过滤器的二进制向量进行遮蔽。最后, 在包含通配符的关键词检索功能的实现上, 该方法通过预先为关键词生成所有通配检索形式。例如, 关键词 flower 的所有通配检索形式包括 flower,*flower,flower*,*lower,...,flowe*,*ower,...,*wer,f*er,fl*r, flo*,*er,f*r,fl*,*r,f* 等, 插入索引, 从而将包含通配符的关键词检索转化为精确匹配检索. 2012 年，Kuzu[18] 等人提出了一个可以在大规模加密数据集上进行相似性查询的安全索引方案。它的基本思想是: 利用局部敏感哈希对数据进行哈希操作, 并使用一个向量记录该数据项, 由哈希结果和对应向量组成哈希桶, 其中哈希结果用作桶标记。为了满足数据安全性的要求, 对桶标记和向量分别进行加密, 所有的加密哈希桶形成一个安全索引，再将加密的原始数据和安全索引存储在云服务器上供合法用户使用。查询时先对关键字进行同样的哈希操作, 然后将哈希结果和索引中的哈希桶一一比较。最后分析并计算碰撞成功的哈希桶中的向量, 返回碰撞次数符合要求的数据项。

2010 年，Wang[19] 等人提出了支持结果排序的单关键字密文检索方案, 该方案利用安全索引来实现检索功能, 以各个检索词的散列值为索引项, 索引项对应的倒排链表内容均被加密保存, 排序功能借助于保序加密技术实现, 服务器直接对密文相关分进行大小比较, 从而实现对结果文档的排序。2011 年，Cao[20] 等人提出了针对多关键词的在密文文件集合上进行排序检索的可搜索加密方案 MRSE, 该方案以内积匹配来分析关键词与文件之间的相关性, 从线性代数的角度解释了关键词与相应文件的对应相似观点, 而且初步解决了在密文上基于多关键词进行排序检索操作的问题。然而服务器在进行检索操作时, 必须对可搜索索引进行线性扫描, 所以在密文上检索文件的效率还是亟待提高。针对 MRSE 存在的失序问题,Xu[21] 等人提出了多关键词排序搜索方案 MKQE, 该方案同样采用向量空间模型表示文档和查询语句, 但对查询语句的向量结构做了改进, 提高了检索结果的排序特性。为提高检索效率,Sun[22] 等人提出了一种改进方案, 该方案为所有文档建立一棵索引树, 树节点为权重向量, 树叶子节点为文档编号, 检索时以向量夹角的大小为排序依据。2016 年，Chen[23] 等人提出了在大数据量环境下支持更多搜索语义并满足快速密文搜索需求的层次聚类方法, 其根据最小相关阈值聚类文档, 将生成的簇划分成子簇, 直到达到最大簇约束。但该方法只达到了线性复杂度, 针对海量密文文档的检索效率仍然不高。

基于 Raykova[24] 等人的工作,PaPPas[25] 等人在 2014 年基于布隆过滤器提出了一个支持范围查询的 SSE 方案，通过将范围查询转化为多关键词的析取查询，可以实现亚线性的查询时间复杂度。然而 Pappas 的方案支持的查询方式较少并且没有扩展性。2015 年，Faber[26] 等人基于 OXT 协议[11] 也提出了一个把范围查询转化为多关键词析取查询的方案，该方案有很好的扩展性而且支持子字符串和通配符查询。

1.3 怎样用 LaTeX

本模板在 Windows + TeXLive2016 + Texsdudio 平台下开发，采用 XeLaTex 编译。虽然之前也开发过一个基于 CTeX 的模板，但是经过多方面比较发现 TeXLive+XeLaTex

处理中文更好，所以基于 CTeX 的模板没有共享。

本模板不能在 CTeX 软件下使用，必须采用 TeXLive，并且编译方式是 XeLaTeX。TeXLive 每年更新一个版本，我用的是 TeXLive2016。文本编辑器可以根据自己的喜好选用，我用的是 Texsdudio，这款开源软件非常不错，推荐大家使用。

本模板的源文件通过主目录下的 main.tex 统一管理，setup 文件夹中存放格式定义和封面、摘要、目录等内容，body 文件夹中存放论文正文章节的源文件，appendix 文件夹中存放附录、致谢和声明等内容。

本模板只提供论文的格式定义，不提供 LaTeX 的详细使用方法。因为 LaTeX 的资源非常丰富，大家可以在网上查找资料和并参与讨论，这样学习效率更高。我关注的两个网站是：`http://bbs.ctex.org/forum.php` 和 `http://www.latexstudio.net`；参考的两本书是 “The Not So Short Introduction to LaTeX 2_ε” 和 “LaTeX2e 完全学习手册”。

1.4 实际显示内容

crap

2 图表公式排版

虽然本模板不讲解 LaTeX 的详细使用方法，但是为了方便大家使用本模板撰写论文，本章对论文写作中经常用到的**图**、**表**、**公式**等内容的排版方法做一个简单介绍。

2.1 图

2.1.1 单幅图

图 2-1 是用 TeXLive 自带的宏包 Tikz 绘制而成，Visio 画不出这么好看的图。

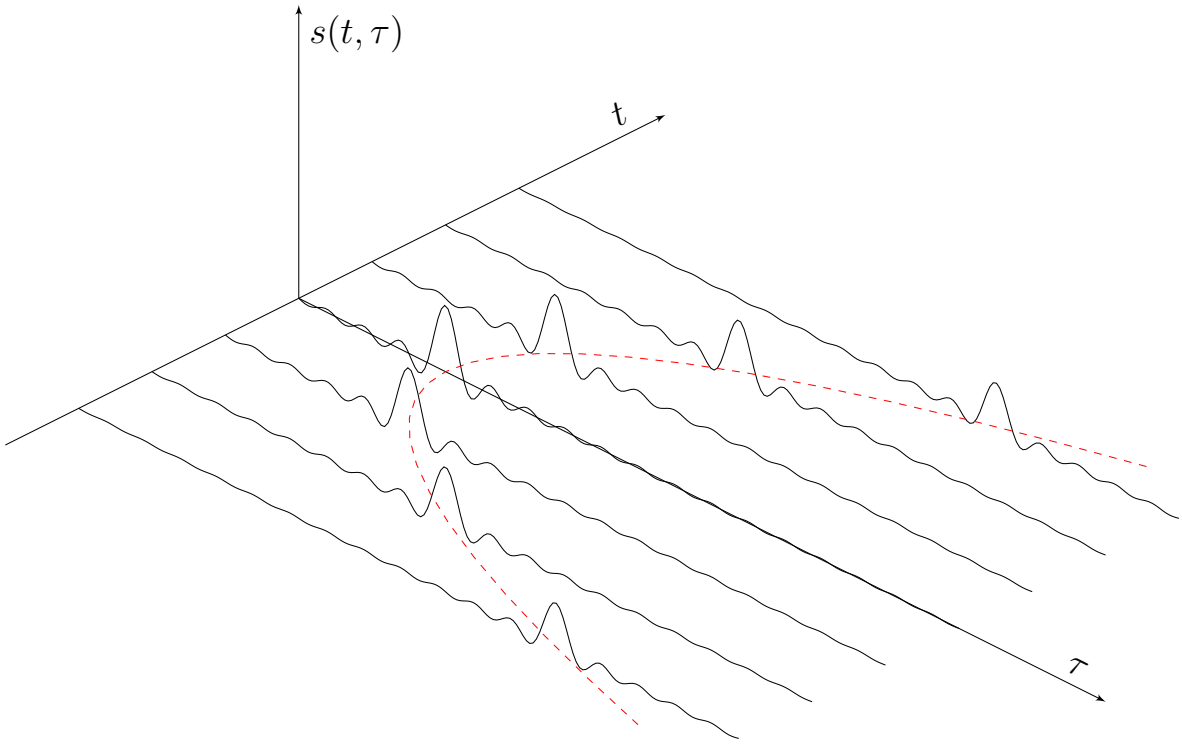

图 2-1 雷达回波信号 (注意：图注是五号字)。

2.1.2 多幅图

如果一幅图中包含多幅子图，每一幅子图都要有图注，并且子图用 (a)、(b)、(c) 等方式编号，如图 2-2 所示。

2.2 表

表格要求采用三线表，与文字齐宽，顶线与底线线粗是 $1\frac{1}{2}$ 磅，中线线粗是 1 磅，如表 2-1 所示[①]。

① 注意：图表中的变量与单位通过斜线 / 隔开。

(a) 灰色的交大校徽

(b) 蓝色的交大校徽

图 2-2 交大校徽

表 2-1 表题也是五号字

Interference	DOA / degree	Bandwidth / MHz	INR / dB
1	−30	20	60
2	20	10	50
3	40	5	40

2.3 公式

2.3.1 单个公式

LaTeX 最强大的地方在于对数学公式的编辑，不仅美观，而且高效。单个公式的编号如式 (2-1) 所示，该式是正态分布的概率密度函数[27]，

$$f_Z(z) = \frac{1}{\pi\sigma^2}\exp\left(-\frac{|z-\mu|^2}{\sigma^2}\right) \tag{2-1}$$

式中：μ 是 Gauss 随机变量 Z 的均值；σ^2 是 Z 的方差。

2.3.2 多个公式

多个公式作为一个整体可以进行二级编号，如式 (2-2) 所示，该式是连续时间 Fourier 变换的正反变换公式[28]，

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}\mathrm{d}t \tag{2-2a}$$

$$x(t)=\int_{-\infty}^{\infty}X(f)e^{j2\pi ft}\mathrm{d}f \tag{2-2b}$$

式中：$x(t)$ 是信号的时域波形；$X(f)$ 是 $x(t)$ 的 Fourier 变换。

如果公式中包含推导步骤，可以只对最终的公式进行编号，例如：

$$\begin{aligned}\mathbf{w}_{\mathrm{smi}}&=\alpha\left[\frac{1}{\sigma_n^2}\mathbf{v}(\theta_0)-\frac{1}{\sigma_n^2}\mathbf{v}(\theta_0)+\sum_{i=1}^{N}\frac{\mathbf{u}_i^H\mathbf{v}(\theta_0)}{\lambda_i}\mathbf{u}_i\right]\\&=\frac{\alpha}{\sigma_n^2}\left[\mathbf{v}(\theta_0)-\sum_{i=1}^{N}\mathbf{u}_i^H\mathbf{v}(\theta_0)\mathbf{u}_i+\sum_{i=1}^{N}\frac{\sigma_n^2\mathbf{u}_i^H\mathbf{v}(\theta_0)}{\lambda_i}\mathbf{u}_i\right]\\&=\frac{\alpha}{\sigma_n^2}\left[\mathbf{v}(\theta_0)-\sum_{i=1}^{N}\frac{\lambda_i-\sigma_n^2}{\lambda_i}\mathbf{u}_i^H\mathbf{v}(\theta_0)\mathbf{u}_i\right]\end{aligned} \tag{2-3}$$

3 参考文献格式

参考文献格式应符合国家标准 GB/T-7714-2005《文后参考文献著录规则》。中国国家标准化管理委员会于 2015 年 5 月 15 日发布了新的标准 GB/T 7714-2015《信息与文献参考文献著录规则》。因为二者的差别非常小，所以采用了新的标准。标准的 BiBTeX 格式网上资源非常多，本模板使用了李泽平开发的版本，该版本提供了多种参考文献的排序规则。学校博士论文规范指定了两种排序方法：一是按照文献的引用顺序进行排序，二是按照作者姓氏加出版年份进行排序。本模板采用第一种排序规则，第二种排序规则的使用方法请参考文献 [29]。

致　谢

致谢中主要感谢导师和对论文工作有直接贡献和帮助的人士和单位。

一般致谢的内容有：

1. 对指导或协助指导完成论文的导师；
2. 对国家科学基金、资助研究工作的奖学金基金、合同单位、资助或支持的企业、组织或个人；
3. 对协助完成研究工作和提供便利条件的组织或个人；
4. 对在研究工作中提出建议和提供帮助的人；
5. 对给予转载和引用权的资料、图片、文献、研究思想和设想的所有者；
6. 对其他应感谢的组织和个人。

致谢言语应谦虚诚恳，实事求是。字数不超过 1000 汉字。

用于双盲评审的论文，此页内容全部隐去。。

参考文献

[1] Li R, Liu A X. Adaptively secure conjunctive query processing over encrypted data for cloud computing[C]. 2017 IEEE 33rd International Conference on Data Engineering (ICDE): volume 1, 2017: 697-708. DOI: 10.1109/ICDE.2017.122.

[2] Dawn Xiaoding Song, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]. Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, 2000: 44-55. DOI: 10.1109/SECPRI.2000.848445.

[3] Goh E J. Secure Indexes [M], 2003.

[4] Bloom B H. Space/time trade-offs in hash coding with allowable errors[J]. Commun. ACM. 1970.

[5] Chang Y C, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data[C]// Ioannidis J, Keromytis A, Yung M. Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 442–455.

[6] Curtmola R, Garay J A, Kamara S, et al. Searchable symmetric encryption: Improved definitions and efficient constructions.[J/OL]. IACR Cryptology ePrint Archive. 2006, 2006:210. http://dblp.uni-trier.de/db/journals/iacr/iacr2006.html#CurtmolaGKO06.

[7] Golle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data[C]// Jakobsson M, Yung M, Zhou J. Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 31–45.

[8] Ballard L, Kamara S, Monrose F. Achieving efficient conjunctive keyword searches over encrypted data[C]// Qing S, Mao W, López J, et al. Information and Communications Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 414–426.

[9] Byun J W, Lee D H, Lim J. Efficient conjunctive keyword search on encrypted data storage system[C]// Atzeni A S, Lioy A. Public Key Infrastructure. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 184–196.

[10] Ryu E, Takagi T. Efficient conjunctive keyword-searchable encryption[C]. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07): volume 1, 2007: 409-414. DOI: 10.1109/AINAW.2007.166.

[11] Cash D, Jarecki S, Jutla C, et al. Highly-scalable searchable symmetric encryption with support for boolean queries[C]// Canetti R, Garay J A. Advances in Cryptology – CRYPTO 2013. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 353–373.

[12] Lai S, Patranabis S, Sakzad A, et al. Result pattern hiding searchable encryption for conjunctive queries[C/OL]. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: Association for Computing Machinery, 2018: 745 – 762. https://doi.org/10.1145/3243734.3243753. DOI: 10.1145/3243734.3243753.

[13] Sun S F, Liu J K, Sakzad A, et al. An efficient non-interactive multi-client searchable encryption with support for boolean queries[C]// Askoxylakis I, Ioannidis S, Katsikas S, et al. Computer Security – ESORICS 2016. Cham: Springer International Publishing, 2016: 154–172.

[14] Wang Y, Wang J, Sun S F, et al. Towards multi-user searchable encryption supporting boolean query and fast decryption[C]// Okamoto T, Yu Y, Au M H, et al. Provable Security. Cham: Springer International Publishing, 2017: 24–38.

[15] Kamara S, Moataz T. Boolean searchable symmetric encryption with worst-case sub-linear complexity[C]// Coron J S, Nielsen J B. Advances in Cryptology – EUROCRYPT 2017. Cham: Springer International Publishing, 2017: 94–124.

[16] Li J, Wang Q, Wang C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]. 2010 Proceedings IEEE INFOCOM, 2010: 1-5. DOI: 10.1109/INFCOM.2010.5462196.

[17] Bösch C, Brinkman R, Hartel P, et al. Conjunctive wildcard search over encrypted data[C]// Jonker W, Petković M. Secure Data Management. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 114–127.

[18] Kuzu M, Islam M S, Kantarcioglu M. Efficient similarity search over encrypted data[C]. 2012 IEEE 28th International Conference on Data Engineering, 2012: 1156-1167. DOI: 10.1109/ICDE.2012.23.

[19] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C]. 2010 IEEE 30th International Conference on Distributed Computing Systems, 2010: 253-262. DOI: 10.1109/ICDCS.2010.34.

[20] Ananthi S, Sendil M S, Karthik S. Privacy preserving keyword search over encrypted cloud data[C]// Abraham A, Lloret Mauri J, Buford J F, et al. Advances in Computing and Communications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 480–487.

[21] Xu Z, Kang W, Li R, et al. Efficient multi-keyword ranked query on encrypted data in the cloud[C]. 2012 IEEE 18th International Conference on Parallel and Distributed Systems, 2012: 244-251. DOI: 10.1109/ICPADS.2012.42.

[22] Sun W, Wang B, Cao N, et al. Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking[C/OL]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. New York, NY, USA: Association for Computing Machinery, 2013: 71–82. https://doi.org/10.1145/2484313.2484322. DOI: 10.1145/2484313.2484322.

[23] Chen C, Zhu X, Shen P, et al. An efficient privacy-preserving ranked keyword search method[J]. IEEE Transactions on Parallel and Distributed Systems. 2016, 27(4):951–963. DOI: 10.1109/TPDS.2015.2425407.

[24] Raykova M, Vo B, Bellovin S M, et al. Secure anonymous database search[C/OL]. Proceedings of the 2009 ACM Workshop on Cloud Computing Security. New York, NY, USA: Association for Computing Machinery, 2009: 115–126. https://doi.org/10.1145/1655008.1655025. DOI: 10.1145/1655008.1655025.

[25] Pappas V, Krell F, Vo B, et al. Blind seer: A scalable private dbms[C]. 2014 IEEE Symposium on Security and Privacy, 2014: 359-374. DOI: 10.1109/SP.2014.30.

[26] Faber S, Jarecki S, Krawczyk H, et al. Rich queries on encrypted data: Beyond exact matches[C]// Pernul G, Y A Ryan P, Weippl E. Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015: 123–145.

[27] Manolakis D G, Ingle V K, Kogon S M. Statistical and Adaptive Signal Processing[M]. Norwood: Artech House, Inc., 2005.

[28] Vetterli M, Kovacevic J, Goyal V K. Foundations of Signal Processing[M]. Cambridge: Cambridge University Press, 2014.

[29] Lee Z. GB/T 7714-2015 参考文献 BiBTeX 样式 [M/OL]. 2016. https://github.com/zepinglee/gbt7714-bibtex-style. DOI: fuck.

附录 A　公式定理证明

附录编号依次编为附录 A，附录 B。附录标题各占一行，按一级标题编排。每一个附录一般应另起一页编排，如果有多个较短的附录，也可接排。附录中的图表公式另行编排序号，与正文分开，编号前加“附录 A-”字样。

本部分内容非强制性要求，如果论文中没有附录，可以省略《附录》。

排版数学定理等环境时最好给环境添加结束符，以明确定理等内容的起止标志，方便阅读。官方模板未对这些内容进行规范，本模板中定义的结束符采用 ◊，例子的结束符采用 ⧫，定理的结束符采用 □，证明的结束符采用 ■。

定义 A.1 (向量空间)： 设 X 是一个非空集合，$\mathbb{F}$ 是一个数域 (实数域 $\mathbb{R}$ 或者复数域 $\mathbb{C}$)。如果在 X 上定义了加法和数乘两种运算，并且满足以下 8 条性质：

1. 加法交换律，$\forall\, x, y \in X$，$x + y = y + x \in X$；
2. 加法结合律，$\forall\, x, y, z \in X$，$(x + y) + z = x + (y + z)$；
3. 加法的零元，$\exists\, 0 \in X$，使得 $\forall\, x \in X$，$0 + x = x$；
4. 加法的负元，$\forall\, x \in X$，$\exists\ -x \in X$，使得 $x + (-x) = x - x = 0$。
5. 数乘结合律，$\forall\, \alpha, \beta \in \mathbb{F}$，$\forall\, x \in X$，$(\alpha\beta)x = \alpha(\beta x) \in X$；
6. 数乘分配律，$\forall\, \alpha \in \mathbb{F}$，$\forall\, x, y \in X$，$\alpha(x + y) = \alpha x + \alpha y$；
7. 数乘分配律，$\forall\, \alpha, \beta \in \mathbb{F}$，$\forall\, x \in X$，$(\alpha + \beta)x = \alpha x + \beta x$；
8. 数乘的幺元，$\exists\, 1 \in \mathbb{F}$，使得 $\forall\, x \in X$，$1x = x$，

那么称 X 是数域 $\mathbb{F}$ 上的一个**向量空间** (linear space)。 ◊

例 A.1 (矩阵空间)： 所有 $m \times n$ 的矩阵在普通矩阵加法和矩阵数乘运算下构成一个向量空间 $\mathbb{C}^{m\times n}$。如果定义内积如下：

$$\langle A, B\rangle = \operatorname{tr}(B^H Q A) = \sum_{i=1}^{n} b_i^H Q a_i \tag{A-1}$$

其中 a_i 和 b_i 分别是 A 和 B 的第 i 列，而 Q 是 Hermite 正定矩阵，那么 $\mathbb{C}^{m\times n}$ 构成一个 Hilbert 空间。 ⧫

定理 A.1 (Riesz 表示定理)： 设 H 是 Hilbert 空间，H^* 是 H 的对偶空间，那么对 $\forall\, f \in H^*$，存在唯一的 $x_f \in H$，使得

$$f(x) = \langle x, x_f\rangle, \qquad \forall\, x \in H \tag{A-2}$$

并且满足 $\|f\| = \|x_f\|$。 □

证明： 先证存在性，再证唯一性，最后正 $\|f\| = \|x_f\|$。 ■

附录 B 算法与代码

对于数学、计算机和电子信息专业，算法和代码也是经常用到的排版技巧。

B.1 算法

算法描述使用 algorithm2e 宏包，效果如算法 B-1 所示。

Input: $\mathbf{x}(k), \quad \mu, \quad \mathbf{w}(0)$
Output: $y(k), \quad \varepsilon(k)$
for $k = 0, 1, \cdots$ **do**
  $y(k) = \mathbf{w}^H(k)\mathbf{x}(k)$ // output signal
  $\varepsilon(k) = d(k) - y(k)$ // error signal
  $\mathbf{w}(k+1) = \mathbf{w}(k) + \mu\varepsilon^*(k)\mathbf{x}(k)$ // weight vector update
end

算法 B-1 LMS 算法详细描述

B.2 代码

源代码使用 listings 宏包，LMS 算法的 Verilog 模块端口声明如代码 B-1 所示。

代码 B-1 空时 LMS 算法 Verilog 模块端口声明

```
module stap_lms
#(
parameter       M               = 4,    // number of antennas
                L               = 5,    // length of FIR filter
                W_IN            = 18,   // wordlength of input data
                W_OUT           = 18,   // wordlength of output data
                W_COEF          = 20    // wordlength of weights
)(
output  signed  [W_OUT-1:0]     y_i,    // in-phase component of STAP output
output  signed  [W_OUT-1:0]     y_q,    // quadrature component of STAP output
output                          vout,   // data valid flag of output (high)
input           [M*W_IN-1:0]    u_i,    // in-phase component of M antennas
input           [M*W_IN-1:0]    u_q,    // quadrature component of M antennas
input                           vin,    // data valid flag for input (high)
input                           clk,    // clock signal
input                           rst     // reset signal (high)
);
```

攻读学位期间取得的研究成果

研究成果包括以下内容：

1. 已发表或已录用的学术论文、已出版的专著/译著、已获授权的专利按参考文献格式列出。
2. 科研获奖，列出格式为：获奖人 (排名情况). 项目名称. 奖项名称及等级, 发奖机构, 获奖时间.
3. 与学位论文相关的其它成果参照参考文献格式列出。
4. 全部研究成果连续编号编排。

样例：

[1] Wei ZY, Tang YP, Zhao WH, et al. Rapid development technique for drip irrigation emitters[J]. RP Journal,UK., 2003, 9(2):104 110 (SCI: 000350930600051; EI: 03187452127).

[2] 魏正英, 唐一平, 卢秉恒. 滴灌管内嵌管状滴头的快速制造方法研究 [J]. 农业工程学报, 2001,17(2):55 58 (EI:01226526279,01416684777).

[3] 姜锡洲. 一种温热外敷药制备方案: 中国,88105607.3[P].1989-07-26.

[4]

用于双盲评审的论文，只列出已发表的学术论文的篇名、发表刊物名称，必须隐去各类论文检索号、期号、卷号、页码；专利号；日期等。

答辩委员会会议决议

论文提出了××××××××××××××××××××××××××××××××××××××。

论文取得的主要创新性成果包括：

1. ××。
2. ××。
3. ××。

论文工作表明作者在××××× 具有 ××××× 知识，具有 ××××× 能力，论文 ××××××××××，答辩 ××××××××××××××。

答辩委员会表决，（× 票/一致）同意通过论文答辩，并建议授予 ××× （姓名）××× （门类）学博士/硕士学位。

1. 填写内容应与学位（毕业）审批材料中答辩委员会决议书一致。
2. 无需签名。
3. 盲审论文仅保留“答辩委员会会议决议”标题。

常规评阅人名单

本学位论文共接受 X 位专家评阅，其中常规评阅人 X 名，名单如下：

王 XX	教授	西安交通大学
李 XX	教授	XXXX 大学
田 XX	教授	XXXX 大学

盲审论文仅保留“常规评阅人名单”标题。

学位论文独创性声明 (1)

本人声明：所呈交的学位论文系在导师指导下本人独立完成的研究成果。文中依法引用他人的成果，均已做出明确标注或得到许可。论文内容未包含法律意义上已属于他人的任何形式的研究成果，也不包含本人已用于其他学位申请的论文或成果。

本人如违反上述声明，愿意承担以下责任和后果：

1. 交回学校授予的学位证书；
2. 学校可在相关媒体上对作者本人的行为进行通报；
3. 本人按照学校规定的方式，对因不当取得学位给学校造成的名誉损害，进行公开道歉；
4. 本人负责因论文成果不实产生的法律纠纷。

论文作者 (签名)：　　日期：　　年　　月　　日

学位论文独创性声明 (2)

本人声明：研究生_____ 所提交的本篇学位论文已经本人审阅，确系在本人指导下由该生独立完成的研究成果。

本人如违反上述声明，愿意承担以下责任和后果：

1. 学校可在相关媒体上对本人的失察行为进行通报；
2. 本人按照学校规定的方式，对因失察给学校造成的名誉损害，进行公开道歉；
3. 本人接受学校按照有关规定做出的任何处理。

指导教师 (签名)：　　日期：　　年　　月　　日

学位论文知识产权权属声明

我们声明，我们提交的学位论文及相关的职务作品，知识产权归属学校。学校享有以任何方式发表、复制、公开阅览、借阅以及申请专利等权利。学位论文作者离校后，或学位论文导师因故离校后，发表或使用学位论文或与该论文直接相关的学术论文或成果时，署名单位仍然为西安交通大学。

论文作者 (签名)：　　日期：　　年　　月　　日

指导教师 (签名)：　　日期：　　年　　月　　日