可验证对称加密搜索问题分析与研究

（申请清华大学工程硕士专业学位论文）

培养单位：计算机科学与技术系
学　　科：计算机技术
申 请 人：朱洁
指导教师：李琦 副研究员

二〇一八年四月

Analysis and Research of Verifiable Searchable Symmetric Encryption

Thesis Submitted to

Tsinghua University

in partial fulfillment of the requirement

for the professional degree of

Master of Engineering

by

Zhu Jie

(Computer Technology)

Thesis Supervisor : Professor Li Qi

April, 2018

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容。

本人保证遵守上述规定。

（保密的论文在解密后应遵守此规定）

作者签名：______________ 导师签名：______________

日　　期：______________ 日　　期：______________

摘　要

云存储的发展使得用户可以方便地存储、获取与分享数据。但与此同时，云存储也带来了很多安全问题，例如，数据隐私泄露等等。对称加密搜索的提出解决了数据隐私泄露问题，同时也保证了数据的可搜索性。通过使用对称加密搜索方案，用户可以在上传数据到云服务器之前，对数据进行加密，同时云服务器可以在用户的加密数据上进行搜索，从而确保数据隐私。

然而，对称加密搜索的假定是云服务器是诚实且好奇的，即云服务器会遵守协议，但现实情况中云服务器往往是不可靠的。为了解决该问题，可验证对称加密搜索技术相应提出，它通过结果验证技术可以到检测云服务器的恶意行为。但是，现有的可验证对称加密搜索方案都不完善，例如，不支持用户数据动态更新，依赖于特定的对称加密搜索方案，只支持单用户读写等等。

针对以上的问题，本文提出了一种通用的可验证对称加密搜索框架，该框架普适于任何加密搜索方案，支持用户数据更新，并且能够同时在单用户和多用户的场景下工作。本文的主要工作和创新点包括：

- 提出了一种单用户场景下的可验证对称加密搜索框架，并在此基础上设计了结果验证算法，该算法能同时保证数据新鲜性和数据完整性。该框架支持用户数据动态更新，并且将验证索引从对称加密搜索方案中解耦，使其可以为任何加密搜索方案提供结果验证功能。
- 提出了一种多用户场景下的可验证对称加密搜索框架。该框架支持单用户写，多用户读，确保了多用户场景下的数据新鲜性，并实现了数据共享场景下的结果验证。
- 本文采用了一个开源数据集作为测试数据，在本地环境对该框架进行了实验测试。安全性分析和实验表明，本文提出的可验证对称加密搜索框架不泄露数据隐私，并且给对称加密搜索方案引入的额外计算开销和通信开销很小，几乎可以忽略不计。

关键词：对称加密搜索，结果验证，云存储

Abstract

Cloud storage allows users to retrieve and share their data conveniently. Meanwhile, cloud storage also brings serious data privacy issues, i.e., the disclosure of private information. In order to ensure data privacy without losing data usability, Searchable Symmetric Encryption (SSE) has been proposed. By using SSE, users can encrypt their data before uploading to cloud services, and cloud services can directly operate and search over encrypted data, which ensures data privacy.

However, most SSE schemes only work with honest-but-curious cloud services that do not deviate from the prescribed protocols. This assumption does not always hold in practice due to the untrusted nature in storage outsourcing. To alleviate the issue, there have been studies on Verifiable Searchable Symmetric Encryption (VSSE), which functions against malicious cloud services by enabling results verification. But to our best knowledge, existing VSSE schemes exhibit very limited applicability, such as only supporting static database, demanding specific SSE constructions, or only working in the single-user model.

In this paper, we proposed a generic verifiable SSE framework in both single-user model and single-writer multiple-reader model, which provides verifiability for any SSE schemes and further supports data updates. In summary, our contributions are three-fold:

- We proposed a verifiable SSE framework in single-user model and designed the result verification algorithms. The framework seperate the verification index from the SSE construction and can provides generic verification for any SSE schemes. The algorithms guaranteed both data freshness and data integrity with support of data updates.
- We proposed the first verifiable SSE framework in the single-writer and multiple-reader model, which ensures data freshness across multiple users and provides result verification under data sharing scenario.
- We implemented our framework in a local enviroment and fed it with an open-source data set. Rigorous analysis and experimental evaluations show that our shceme is secure and introduces small overhead for result verification.

Key words: Searchable Symmetric Encryption; Result Verification; Cloud Storage

目　录

主要符号对照表

SSE	加密搜索 (Searchable Symmetric Encryption)
VSSE	可验证加密搜索 (Verifiable Searchable Symmetric Encryption)
MPT	默克尔帕特里夏树 (Merkle Patricia Tree)
IH	增量哈希 (Incremental Hash)
$\mathcal{W}$	关键字集合
$\|W\|$	关键字集合大小
w_i	关键字，其中 $i \in \{1, \cdots, \|W\|\}$
$\mathcal{D}$	明文文件集合
D_{w_i}	包含关键字 w_i 的明文文件集合
$\mathcal{C}$	密文文件集合
C_{w_i}	包含关键字 w_i 的密文文件集合
d	明文文件
c	密文文件
W_d	文件 d 包含的关键字集合
τ	搜索令牌
λ	验证索引
π	鉴别符

第 1 章　绪论

1.1　研究背景及选题意义

云存储使得用户可以随时随地地存取数据，并且极大地方便了用户之间的数据共享，降低了维护数据的成本[1–7]。但与此同时，云存储也带来了许多安全性问题，例如，数据丢失，数据隐私泄露等等。总体来说，云存储带来的安全性问题可以分为以下两类：

- 可用性问题。要求云服务器保证数据不丢失，用户可以将云端作为数据中枢进行数据备份和同步。目前，一般的云服务提供商都采用了多副本的方式保障数据的可用性，即将数据的多个副本分别写入其他的存储节点，当一个节点发生故障时，其他节点上的数据继续提供服务，同时通过其他节点中的数据副本，快速恢复故障节点上丢失的数据。目前，针对数据可用性的相关学术研究包括数据拥有证明 (Proof of Data Possession, PDP)[2,8–10] 以及数据可恢复性证明 (Proof of Retrievability, PoR)[1,5,11]。
- 隐私性问题。要求云服务器保证数据的隐私并且不泄露数据。目前，云服务提供商一般采用数据加密方式对隐私数据进行保护，但数据加密往往会导致数据可用性的降低，例如数据失去可搜索性。因此加密搜索 (Searchable Encryption, SE) 应运而生。加密搜索技术主要分为两类，一是对称加密搜索 (Searchable Symmetric Encryption, SSE)[12–16]，二是公钥加密搜索 (Public Key Encryption with Keyword Search, PEKS)[17]。

加密搜索的提出，使得用户可以在上传数据给云服务器之前，对其进行加密，并且使得云服务器可以在加密数据上进行搜索。从而既保证了数据隐私性，又保证了数据的可搜索性。目前，由于效率问题，应用较为广泛的为对称加密搜索技术。然而，大部分的对称加密搜索方案都基于服务器是诚实且好奇的假设[13–15]，即服务器会遵循协议但是可以从用户的查询中推断相关信息。这种假设在实际应用场景中往往是不成立的。因为云服务器可能会因为外部攻击，内部配置错误，软件错误等等问题而导致其违反原有协议[7,28]。这种协议违反导致的最常见问题就是服务器返回的搜索结果不完整，例如，云服务器有可能为了节省计算开销和通信开销而返回少量搜索结果给用户，甚至有可能不返回搜索结果给用户。

为了解决该问题，可验证对称加密搜索技术也相应提出[3,22–28]。可验证对称加密搜索技术允许用户对搜索结果进行验证，来检测服务器的不诚信行为，保障了加密搜索的正确性。然而，据我们所知，现有的可验证对称加密搜索方案都是不完

善的。例如，有的方案[22,24–26] 不支持数据更新，只能作用在静态数据库中，数据库若有变化则需要重建整个索引。有的方案[3,23,27] 无法防止服务器故意返回空结果来规避结果验证。特别需要说明的是，以上这些方案[3,23,27] 在搜索关键字在数据库中不存在时，是不返回任何搜索结果的，这就导致了服务器可以对任意关键字返回空结果来规避结果验证，除非用户在本地保留数据库的所有关键字集合。另外，大部分的可验证对称加密搜索方案[3,22–28] 仅仅支持在单用户场景下工作，即用户自己写自己读的场景，而现实情况中，数据往往有共享需求，即一方写多方读。表格 1.1比较了现有的可验证对称加密搜索方案。

1.2　本文的主要内容

1.3　本文的结构安排

表 1.1　Comparison with existing typical verifiable SSE schemes.

	Dynamism	Three-party[1]	Freshness Verify[2]	Integrity Verify[3]	Prove Efficiency[4]
KPR11[3]	✓	×	✓	×	$O(\|W\|)$
KO12[22]	×	×	-	×	$O(n)$
CG12[25]	×	×	-	✓	$O(log(\|W\|))$
KO13[23]	✓	×	✓	×	$O(n)$
SPS14[27]	✓	×	✓	×	$min\{\alpha + log(N), rlog^3(N)\}$
CYGZR15[26]	×	×	-	×	$O(\|W\|) + O(r)$
BFP16[28]	✓	×	✓	✓	$O(r)$
OK16[24]	×	×	-	✓	$O(r)$
我们的方案	✓	✓	✓	✓	$O(log(\|W\|))$

[1] Three-party means whether the scheme supports search result verification for an SSE scheme with three parties, i.e., data owners, servers, and users.

[2] Note that, '×' represents the requirements which are not implemented, while '-' means the requirements which are not required. Specifically, the static verifiable SSE schemes do not have the problem of data freshness attacks, and thus the existing schemes[22,24–26] do not require data freshness verification.

[3] We consider various data integrity attacks, especially the attacks that servers can intentionally returns an empty result to evade search result verification.

[4] The prove efficiency refers to the cost of operations for search result verification. For some selected non-generic schemes[22,23,25–27], their prove efficiency is equivalent to their encrypted search efficiency. Here, n indicates the number of total files, $|W|$ means the number of all keywords, r means the number of files which contain the specific keyword, α means the number of times this keyword was historically added to the collection[27], and N means the total number of document and keyword pairs.

[5] A generic VSSE scheme means that the verifiable design can provide result verification for any SSE schemes, while a non-generic scheme only works for a particular SSE construction.

第 2 章　相关研究综述

现有的 CS2 论文 [5] 提出了搜索鉴别符方案，该方案利用了默克尔树（Merkle Hash Tree，MHT）来实现了对数据完整性的验证，然而该方案并没有考虑到服务器返回空结果来规避结果验证的情况。Kurosawa 等人提出了一系列可验证加密搜索方案 [6][8][12]，然而他们的方案要么在搜索效率上接近 O(n)，不适用于大型数据库，要么只支持静态数据库。除了 Kurosawa 等人的方案，其他还有许多只支持静态数据库的方案 [7][10][13]。虽然 Stefanov 等人的方案 [9] 通过消息验证码（Message Authenticated Code，MAC）实现了动态数据库下的可验证搜索，然而他们的方案仍然没有考虑到服务器返回空结果的情况。Bost 等人提出的方案是目前为止最完善的 [11]，但他们的方案在搜索时需要和服务器有两轮通信才能进行验证，无法并行进行验证，并且他们的方案同样也不支持多用户情况下的验证。各个方案的对比情况如表格 1 所示。表格 1 现有的可验证加密搜索方案比较动态性多用户防御重放攻击防御数据完整性攻击验证效率

2.2 可验证的非对称加密搜索第一个可验证的非对称加密搜索方案 [18] 由 Zheng 等人提出，他们的方案采用了基于属性的关键字（Attribute-based keyword，ABK），但是他们的方案也只适用于数据库静态的情况。基于他们的工作，Liu 等人又提出了一个更高效的可验证非对称加密搜索方案 [19]，然而，由于非对称加密本身的限制，他们的方案必不可少地需要引入一个可信第三方。2.3 不可验证的多用户加密搜索 Curtmola 等人在 2006 年即提出了一个基于广播加密的多用户加密搜索方案 [2]，该方案允许数据拥有者将数据分享给其他用户，并且数据拥有者具有对用户的访问控制权限，可以随时撤销或者新增用户。Jerecki 等人随后又提出了一个基于 Oblivious Cross Tag 的加密搜索方案 [21]，然而该方案需要数据拥有者和数据用户频繁的交互。2.4 总结综上所述，现有的可验证加密搜索方案都不能满足多用户场景下的安全性保证，并且现有的方案无法完善地解决重放攻击和数据完整性攻击。这需要我们设计合理的机制来防御多用户场景下重放攻击，并且需要我们利用新型的数据结构来完善对数据完整性攻击的防御，尤其是防御服务器返回空结果来规避结果验证的情况。

The scheme proposed by Kamara et al. [5] constructed a Merkle Tree by storing the key and value pairs in its leaf node, where the key was the encrypted keyword and the value was the encrypted data set that contained the keyword. A data user (aka data owner) only kept the root hash of the Merkle Tree. By reconstructing a root hash through the path of the target nodes, the user can check the integrity of the search result. However, they did not clearly state how to handle the situation that the server maliciously returned an empty result set. Unfortunately, their approach cannot detect such attacks. The key reason is that there is no path that matches a non-existent keyword of the Merkle Tree. One naïve way to address this issue is that they can store the results (including empty sets) of the entire keyword space to the tree, which is not scalable. In addition, this approach is not dynamic friendly. It may require rebuilding the entire tree after data update. Kurosawa et al. [8] leveraged Message Authenticated Code (MAC) to ensure data integrity and utilizes RSA accumulator to ensure data freshness during data updates. However, the existing study [12] showed that users in [8] required maintaining all keywords in the datasets to detect cheating of servers. It introduces significant overhead for users to maintain a large set of keywords. Therefore, paper [12] proposed a no-dictionary VSSE scheme, which means users do not need to keep the keywords set as a dictionary. However, their scheme only works in the static setting and does not consider data update scenarios. Stefanov et al. [9] also used MAC and timestamp to ensure data integrity and freshness. However, they were still unable verify an empty search result unless the data owner maintained all keywords locally. In summary, verification on the three-party model (across multiple users) should allow users to verify an empty result in addition to verification of integrity and freshness of search results. Meanwhile, it is desirable that users do not need to maintain a large set of keywords locally for the verification. We clarified this issue in Section 1.

2.1 Related Work

Secure Cloud Storage Scheme. Verifiable cloud storage services have been extensively studied, e.g., Proof of Data Possession (PDP)[2,8–10] and Proof of Retrievability (POR)[1,5,11]. These schemes mainly focused on verifying the integrity of data stored in cloud services and enable restoring data blocks if they are corrupted. However, they did not ensure the integrity of search results, which is the focus of VSSE. Authenticated data structures are used by a set of searching algorithms to verify the integrity of data blocks stored on an untrusted server. Several schemes have been proposed, e.g., Merkle Tree[18], authenticated hash table[19], and authenticated skip list[20,21]. Merkle Tree is the most common structure used to verify data integrity. However, Merkle Tree cannot flexible support data update. Moreover, the current verification scheme[3] built upon Merkle Tree did not store keyword information in its intermediate node and thus it is not suitable for keyword related searches. An authenticated hash table enabled by the RSA accumulator can be used to verify search results as well. Unfortunate, it has low efficiency in searching and update operations. For example, the search delay of the authenticated hash table is in millisecond level, while that of is in microsecond level. Skip list used a multilayer linked list to improve its search efficiency, but the storage overhead is much higher than a tree structure if the keyword information is required in the search path.

Verifiable Searchable Symmetric Encryption. The CS2 scheme[3] enabled users to verify the search result by using dynamic search authenticators, but their scheme cannot prevent the attacks that the server maliciously replies an empty result. Recently Kurosawa et al.[22–24] proposed a few verifiable SSE schemes. However, their schemes either have low search efficiency, or do not support verification upon file update. Kurosawa et al.[22] required linear search in SSE and did not support dynamic file update. Their extension[23] achieved dynamic updating but the search complexity was beyond linear time. Recently, Ogata et al.[24] presented a generic verifiable scheme. It transforms any SSE scheme to a *no-dictionary* verifiable SSE scheme that did not require the users to keep the keyword set. However, it was still a static approach, which shared the similar shortcoming with[25][26]. Although the verifiable scheme proposed by Stefanov et al.[27] achieved verifiability by leveraging message authenticated code, it cannot easily detect the data integrity attacks when the server intentionally returned an empty result. Bost et al.[28] presented a generic verifiable dynamic SSE scheme and combined it with the SSE scheme proposed by Stefanov et al.[27]. Yet, their scheme required two round communications for result verification and did not enable verification in the setting of multiple users. Our scheme is a generic verifiable SSE scheme that can work with three-party model, which can be more readily deployed in practice. In particular, it enables search result verification under file update with only one round of communication.

Verifiable Public Key Encryption with Keyword Search. The first verifiable attribute-based keyword search (VABKS) was proposed by Zheng et al.[29]. Similar to the existing SSE schemes above, VABKS only focused on search based on static encrypted data. Liu et.al[30] proposed a more efficient construction based on VABKS, and Sun et.al[7] also provided a verifiable scheme VCKS that support conjunctive keyword search. However, due to the limitations of asymmetric encryption schemes, both of the above schemes require an additional trusted authority.

Multi-User Searchable Encryption. A few of non-verifiable multi-user schemes have been proposed[13,31–33]. Curtmola et al.[13] first proposed a multi-user SSE scheme based on broadcast encryption. Yang et al.[31] proposed a multi-user searchable encryption scheme by leveraging a bilinear map. However, the search delay of the scheme is proportional to the size of the database, which is not suitable for large-scale databases. Jarecki et al.[32] designed a multi-user scheme by using Oblivious Cross-Tags (OXT) protocol. However, their scheme required frequent communication between data owners and the users, which incured unnecessary communication overheads. Recently, Sun et al.[33] proposed a non-interactive multi-user searchable encryption schemes that reduced the interactions between data owner and users. However, the scheme did not support search under data update.

第 3 章　单用户下的可验证对称加密搜索方案研究

第 4 章　多用户下的可验证对称加密搜索方案研究

第 5 章　总结与展望

参考文献

[1] Juels A, Kaliski Jr B S. Pors: Proofs of retrievability for large files[C]//Proc. of CCS. [S.l.: s.n.], 2007: 584–597.

[2] Ateniese G, Di Pietro R, Mancini L V, et al. Scalable and efficient provable data possession[C]// Proc. of Security and privacy in communication netowrks (SecureComm). [S.l.: s.n.], 2008.

[3] Kamara S, Papamanthou C, Roeder T. Cs2: A semantic cryptographic cloud storage system[R]. [S.l.]: Tech. Rep. MSR-TR-2011-58, Microsoft Technical Report (May 2011), http://research. microsoft. com/apps/pubs, 2011.

[4] Wang Q, Wang C, Ren K, et al. Enabling public auditability and data dynamics for storage security in cloud computing[J]. IEEE TPDS, 2011, 22(5): 847–859.

[5] Stefanov E, van Dijk M, Juels A, et al. Iris: A scalable cloud file system with efficient integrity checks[C]//Proc. of Annual Computer Security Applications Conference (ACSAC). [S.l.: s.n.], 2012.

[6] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption[C]//Proc. of International Conference on Financial Cryptography and Data Security(FC). [S.l.: s.n.], 2013.

[7] Sun W, Liu X, Lou W, et al. Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data[C]//Proc. of INFOCOM. [S.l.: s.n.], 2015.

[8] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores[C]//Proc. of CCS. [S.l.: s.n.], 2007.

[9] Erway C C, Küpçü A, Papamanthou C, et al. Dynamic provable data possession[J]. ACM TISSEC, 2015, 17(4): 15.

[10] Zhu Y, Hu H, Ahn G J, et al. Cooperative provable data possession for integrity verification in multicloud storage[J]. IEEE TPDS, 2012, 23(12): 2231–2244.

[11] Bowers K D, Juels A, Oprea A. Proofs of retrievability: Theory and implementation[C]//Proc. of the workshop on Cloud computing security (SCC). [S.l.: s.n.], 2009.

[12] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]//Proc. of S&P. [S.l.: s.n.], 2000.

[13] Curtmola R, Garay J, Kamara S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[J]. Journal of Computer Security, 2011, 19(5): 895–934.

[14] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption[C]//Proc. of CCS. [S.l.: s.n.], 2012: 965–976.

[15] Cash D, Jaeger J, Jarecki S, et al. Dynamic searchable encryption in very-large databases: Data structures and implementation.[C]//NDSS: volume 14. [S.l.: s.n.], 2014: 23–26.

[16] Wang Q, He M, Du M, et al. Searchable encryption over feature-rich data[J]. IEEE Transactions on Dependable and Secure Computing, 2016.

[17] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]// Proc. of EUROCRYPT. [S.l.: s.n.], 2004.

[18] Merkle R C. A digital signature based on a conventional encryption function[C]//Proc. of EUROCRYPT. [S.l.: s.n.], 1987.

[19] Papamanthou C, Tamassia R, Triandopoulos N. Authenticated hash tables[C]//Proc. of CCS. [S.l.: s.n.], 2008.

[20] Pugh W. Skip lists: a probabilistic alternative to balanced trees[J]. Communications of the ACM, 1990, 33(6): 668–676.

[21] Goodrich M T, Tamassia R, Schwerin A. Implementation of an authenticated dictionary with skip lists and commutative hashing[C]//Proc. of DARPA Information Survivability Conference & Exposition (DISCEX). [S.l.: s.n.], 2001.

[22] Kurosawa K, Ohtaki Y. Uc-secure searchable symmetric encryption[C]//Proc. of International Conference on Financial Cryptography and Data Security (FC). [S.l.: s.n.], 2012.

[23] Kurosawa K, Ohtaki Y. How to update documents verifiably in searchable symmetric encryption [C]//Proc. of International Conference on Cryptology And Network Security (CANS). [S.l.: s.n.], 2013.

[24] Ogata W, Kurosawa K. Efficient no-dictionary verifiable sse[J]. IACR Cryptology ePrint Archive, 2016, 2016: 981.

[25] Chai Q, Gong G. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers[C]//Proc. of International Conference on Communications (ICC). [S.l.: s.n.], 2012.

[26] Cheng R, Yan J, Guan C, et al. Verifiable searchable symmetric encryption from indistinguishability obfuscation[C]//Proc. of AsiaCCS. [S.l.: s.n.], 2015.

[27] Stefanov E, Papamanthou C, Shi E. Practical dynamic searchable encryption with small leakage [C]//Proc. of NDSS. [S.l.: s.n.], 2014.

[28] Bost R, Fouque P A, Pointcheval D. Verifiable dynamic symmetric searchable encryption: Optimality and forward security.[J]. IACR Cryptology ePrint Archive, 2016, 2016: 62.

[29] Zheng Q, Xu S, Ateniese G. Vabks: verifiable attribute-based keyword search over outsourced encrypted data[C]//Proc. of INFOCOM. [S.l.: s.n.], 2014.

[30] Liu P, Wang J, Ma H, et al. Efficient verifiable public key encryption with keyword search based on kp-abe[C]//Proc. of Broadband and Wireless Computing, Communication and Applications (BWCCA). [S.l.: s.n.], 2014.

[31] Yang Y, Bao F, Ding X, et al. Multiuser private queries over encrypted databases[J]. International Journal of Applied Cryptography, 2009, 1(4): 309–319.

[32] Jarecki S, Jutla C, Krawczyk H, et al. Outsourced symmetric private information retrieval[C]// Proc. of CCS. [S.l.: s.n.], 2013.

[33] Sun S F, Liu J K, Sakzad A, et al. An efficient non-interactive multi-client searchable encryption with support for boolean queries[C]//Proc. of ESORICS. [S.l.: s.n.], 2016.

致　谢

衷心感谢导师 xxx 教授和物理系 xxx 副教授对本人的精心指导。他们的言传身教将使我终生受益。

在美国麻省理工学院化学系进行九个月的合作研究期间，承蒙 xxx 教授热心指导与帮助，不胜感激。感谢 xx 实验室主任 xx 教授，以及实验室全体老师和同学们的热情帮助和支持！本课题承蒙国家自然科学基金资助，特此致谢。

感谢 LaTeX 和 ThuThesis[?]，帮我节省了不少时间。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：____________ 日　期：____________

个人简历、在学期间发表的学术论文与研究成果

个人简历

xxxx 年 xx 月 xx 日出生于 xx 省 xx 县。

xxxx 年 9 月考入 xx 大学 xx 系 xx 专业，xxxx 年 7 月本科毕业并获得 xx 学士学位。

xxxx 年 9 月免试进入 xx 大学 xx 系攻读 xx 学位至今。

发表的学术论文

[1] Yang Y, Ren T L, Zhang L T, et al. Miniature microphone with silicon- based ferroelectric thin films. Integrated Ferroelectrics, 2003, 52:229-235. (SCI 收录, 检索号:758FZ.)

[2] 杨轶, 张宁欣, 任天令, 等. 硅基铁电微声学器件中薄膜残余应力的研究. 中国机械工程, 2005, 16(14):1289-1291. (EI 收录, 检索号:0534931 2907.)

[3] 杨轶, 张宁欣, 任天令, 等. 集成铁电器件中的关键工艺研究. 仪器仪表学报, 2003, 24(S4):192-193. (EI 源刊.)

[4] Yang Y, Ren T L, Zhu Y P, et al. PMUTs for handwriting recognition. In press. (已被 Integrated Ferroelectrics 录用. SCI 源刊.)

[5] Wu X M, Yang Y, Cai J, et al. Measurements of ferroelectric MEMS microphones. Integrated Ferroelectrics, 2005, 69:417-429. (SCI 收录, 检索号:896KM)

[6] 贾泽, 杨轶, 陈兢, 等. 用于压电和电容微麦克风的体硅腐蚀相关研究. 压电与声光, 2006, 28(1):117-119. (EI 收录, 检索号:06129773469)

[7] 伍晓明, 杨轶, 张宁欣, 等. 基于 MEMS 技术的集成铁电硅微麦克风. 中国集成电路, 2003, 53:59-61.

研究成果

[1] 任天令, 杨轶, 朱一平, 等. 硅基铁电微声学传感器畴极化区域控制和电极连接的方法: 中国, CN1602118A. (中国专利公开号)

[2] Ren T L, Yang Y, Zhu Y P, et al. Piezoelectric micro acoustic sensor based on ferroelectric materials: USA, No.11/215, 102. (美国发明专利申请号)