**CHAPTER-2**

**INTRODUCTION**

With the rapid development of science and technology, enterprises or individual users increasingly rely on storing a large number of data documents on cloud servers in order to share data quickly and remotely [1]. However, with the increasing demand, the cost of cloud server storage increases, the efficiency of search decreases, and privacy protection has become a focus of research [2]. In most of the existing cipher-text sorting retrieval methods, KNN (K Nearest Neighbor) technology is used to create indexes supporting cipher-text retrieval [3]–[5]. In the process of massive data encryption search, most of the search encryption schemes have high time complexity and large storage space, which are closely related to the encrypted key, the document index and query request dimensions [6], [7]. Reducing high dimensional data encryption is a solution to improve search efficiency [8]. Some researchers try to study how to enrich the flexibility of retrieval [9], [10], however they still cannot meet the retrieval requirements of a large number of data, and they cannot sort and filter useful data for authorized users. Therefore, in the face of different user needs, it is urgent to find a scheme that can not only guarantee privacy, but also improve retrieval efficiency and ensure query accuracy.

* 1. **LITERATURE SURVEY**

1. **Title: One-Time, Oblivious, and Unlinkable Query Processing Over Encrypted Data on Cloud**

**Author:** [Yifei Chen](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Yifei-Chen),  [Meng Li](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Meng-Li), [Shuli Zheng](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Shuli-Zheng),  [Donghui Hu](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Donghui-Hu), [Chhagan Lal](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Chhagan-Lal) &  [Mauro Conti](https://link.springer.com/chapter/10.1007/978-3-030-61078-4_20#auth-Mauro-Conti)

**ABSTRACT**: Searchable Symmetric Encryption aims at making possible searching over an encrypted database stored on an untrusted server while keeping privacy of both the queries and the data, by allowing some small controlled leakage to the server. Recent work shows that dynamic schemes -- in which the data is efficiently updatable -- leaking some information on updated keywords are subject to devastating adaptative attacks breaking the privacy of the queries. The only way to thwart this attack is to design forward private schemes whose update procedure does not leak if a newly inserted element matches previous search queries. This work proposes Sophos as a forward private SSE scheme with performance similar to existing less secure schemes, and that is conceptually simpler (and also more efficient) than previous forward private constructions. In particular, it only relies on trapdoor permutations and does not use an ORAM-like construction. We also explain why Sophos is an optimal point of the security/performance trade-off for SSE.

# Title: Top-k Query Processing on Encrypted Databases with Strong Security Guarantees

**Author**: [Xianrui Meng](https://ieeexplore.ieee.org/author/37086504706); [Haohan Zhu](https://ieeexplore.ieee.org/author/37086502273); [George Kollios](https://ieeexplore.ieee.org/author/37276300000)

**ABSTRACT**: Concerns about privacy in outsourced cloud databases have grown recently and many efficient and scalable query processing methods over encrypted data have been proposed. However, there is very limited work on how to securely process top-k ranking queries over encrypted databases in the cloud. In this paper, we propose the first efficient and provably secure top-k query processing construction that achieves adaptive CQA security. We develop an encrypted data structure called EHL and describe several secure sub-protocols under our security model to answer top-k queries. Furthermore, we optimize our query algorithms for both space and time efficiency. Finally, we empirically evaluate our protocol using real world datasets and demonstrate that our construction is efficient and practical.

# Title: Adaptively Secure Conjunctive Query Processing over Encrypted Data for Cloud Computing

# Author: [Rui Li](https://ieeexplore.ieee.org/author/37071988400); [Alex X. Liu](https://ieeexplore.ieee.org/author/37276667400)

# ABSTRACT: This paper concerns the fundamental problem of processing conjunctive queries that contain both keyword conditions and range conditions on public clouds in a privacy preserving manner. No prior Searchable Symmetric Encryption (SSE) based privacy-preserving conjunctive query processing scheme satisfies the three requirements of adaptive security, efficient query processing, and scalable index size. In this paper, we propose the first privacy preserving conjunctive query processing scheme that satisfies the above requirements. To achieve adaptive security, we propose an Indistinguishable Bloom Filter (IBF) data structure for indexing. To achieve efficient query processing and structure indistinguishability, we propose a highly balanced binary tree data structure called Indistinguishable Binary Tree (IBtree). To optimize searching efficiency, we propose a traversal width minimization algorithm and a traversal depth minimization algorithm. To achieve scalable and compact index size, we propose an IBtree space compression algorithm to remove redundant information in IBFs. We formally prove that our scheme is adaptive secure using a random oracle model. The key contribution of this paper is on achieving conjunctive query processing with both strong privacy guarantee and practical efficiency in terms of both speed and space. We implemented our scheme in C++, evaluated and compared its performance with KRB [24] for keyword queries and PBtree [32] for range queries on two real-world data sets. Experimental results show that our scheme is fast and scalable (in milliseconds).

# Title: Secure KNN Queries over Encrypted Data: Dimensionality Is Not Always a Curse

# Author: [u Lei](https://ieeexplore.ieee.org/author/37086115533); [Alex X. Liu](https://ieeexplore.ieee.org/author/37276667400); [Rui Li](https://ieeexplore.ieee.org/author/37071988400)

# ABSTRACT: The fast-increasing location-dependent applications in mobile devices are manufacturing a plethora of geospatial data. Outsourcing geospatial data storage to a powerful cloud is an economical approach. However, safeguarding data users' location privacy against the untrusted cloud while providing efficient location-aware query processing over encrypted data are in conflict with each other. As a step to reconcile such conflict, we study secure k nearest neighbor (SkNN) queries processing over encrypted geospatial data in cloud computing. We design 2D SkNN (2DSkNN), a scheme achieves both strong provable security and high-efficiency. Our approach employs locality sensitive hashing (LSH) in a dimensional-increased manner. This is a counter-intuitive leverage of LSH since the traditional usage of LSH is to reduce the data dimensionality and solve the so-called "curse of dimensionality" problem. We show that increasing the data dimensionality via LSH is indeed helpful to tackle 2DSkNN problem. By LSH-based neighbor region encoding and two-tier prefix-free encoding, we turn the proximity test to be sequential keywords query with a stop condition, which can be well addressed by any existing symmetric searchable encryption (SSE) scheme. We show that 2DSkNN achieves adaptive indistinguishability under chosen-keyword attack (IND2-CKA) secure in the random oracle model. A prototype implementation and experiments on both real-world and synthetic datasets confirm the high practicality of 2DSkNN.

# Title:  SecEQP: A Secure and Efficient Scheme for SkNN Query Problem Over Encrypted Geodata on Cloud

**Author**: [Xinyu Lei](https://ieeexplore.ieee.org/author/37086115533); [Alex X. Liu](https://ieeexplore.ieee.org/author/37276667400); [Rui Li](https://ieeexplore.ieee.org/author/37071988400); [Guan-Hua Tu](https://ieeexplore.ieee.org/author/37085714535)

**ABSTRACT:** Nowadays, location-based services are proliferating and being widely deployed. For example, a Yelp user can obtain a list of the recommended restaurants near his/her current location. For some small or medium location service providers, they may rely on commercial cloud services, e.g., Dropbox, to store the tremendous geospatial data and deal with a number of user queries. However, it is challenging to achieve a secure and efficient location-based query processing over encrypted geospatial data stored on the cloud. In this paper, we propose the Secure and Efficient Query Processing (SecEQP) scheme to address the secure k nearest neighbor (SkNN) query problem. SecEQP employs the projection function-based approach to code neighbor regions of a given location. Given the codes of two locations, the cloud server only needs to compare whether codes equal or not to check the proximity of the two locations. The codes are further embedded into an indistinguishable Bloom filter tree to build a secure and efficient index. The security of SecEQP is formally proved in the random oracle model. We further prototype SecEQP scheme and evaluate its performance on both real-world and synthetic datasets. Our evaluation results show that SecEQP is a highly efficient approach, e.g., top-10 NN query over 1 million datasets only needs less than 40 msec to get queried results.