**CHAPTER-2**

**INTRODUCTION**

OUR data are increasingly stored in cloud servers (CSs) for a range of reasons, such as lower costs of data management, higher quality of service, and ability to access our data anywhere anytime using any computing device. In some cases, data (on our mobile devices and laptops) are being outsourced to the CSs (e.g., iCloud or OneDrive) by default. There are known security and privacy issues associated with the outsourcing of data, such as the cloud service provider (CSP) getting access to user contents without their explicit permission. This reinforces the importance of searchable encryption (SE), a cryptographybased scheme that enables searching in the ciphertext domain without leaking any information to untrusted servers. There are many different SE schemes, with varying functionalities (e.g., keyword searches and similarity searches). Range searches are another common function in databases that focuses on numeric comparisons, for example to locate users between 20 and 40 years old. To achieve better efficiency in range searches, the data may be processed to fit some specific data structure (e.g., B-tree), in which the data are stored in order. This is easy to achieve in the plaintext domain, but not the case when databases are encrypted. First, the numeric comparisons cannot be made in the encrypted environment due to the lack of semantic information. Also, it is impractical to enumerate all possible cases for the entire range in a search request in order to check the equality. Second, the order between different data records is also sensitive information. In other words, the data owner (DO) generally does not want the CS to know about the order between different data records, and the index should not expose the order information prior to searching. Therefore, it is challenging to conduct range search in the ciphertext domain. In 2016, Zhang et al. [1] proposed the file-inject attacks on SE schemes, and many forward secure solutions were proposed to mitigate such an attack. A forward secure scheme guarantees that the update operation does not leak the relationship between the updating keywords and the previous documents. That is to say, the cloud cannot learn whether entries that have been updated recently contain some specific keywords. However, all the forward secure schemes discussed so far support only keyword search rather than range search. In this project, we present the formal definition for forward privacy in range searches, and then propose an efficient, accurate, and forward secure (EAFS) SE scheme that satisfies this definition. To be specific, our scheme achieves secure range search in a single CS model, and the accurate results can be obtained without redundant interactions and postprocessing operations. The search phase consists of two parts. The first part is to find the dataset that completely meets the search request, and the second part is to find the dataset that partially meets the search request and then compare to return the correct results. Thus, the complexity of the search is related to the size of the datasets mentioned above. Both order information and similarity information are hidden before a search is conducted, and forward privacy is guaranteed when the data records are updated. Furthermore, we also compare our proposed scheme with Wu et al.’s state-of-the-art tree-based SE scheme (Serve DB). Based on the comparison, we observe that our scheme achieves both accuracy and forward privacy, unlike Serve DB. Findings from the experiments also demonstrate that the computational cost of our scheme is less than that of Serve DB. Table Ⅰ gives a comparative summary of our scheme and prior art. The following summarizes the article.

1) We propose the first formal definition of forward privacy in secure range searches.

2) We design an EAFS SE scheme that supports secure range searches in encrypted databases. This is the first scheme that simultaneously achieves efficiency, accuracy, and forward security.

3) We demonstrate that the EAFS is secure under the semi honest model by utilizing the simulation-based method.

4) We implement the EAFS and evaluate its performance on Microsoft Azure CSs. A comparison with another state of-the-art tree-based SE scheme demonstrates that our scheme achieves both efficiency, accuracy and supports forward privacy

* 1. **LITERATURE SURVEY**

# Title: Forward Secure Searchable Encryption

# Author: Raphael Bost [Authors Info & Claims](https://dl.acm.org/doi/abs/10.1145/2976749.2978303#pill-authors__contentcon)

**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.

# 2.Title: Practical Backward-Secure Searchable Encryption from Symmetric Puncturable Encryption

**Author**: Shi-Feng Sun, Xingliang Yuan, Joseph K. Liu, [Ron Steinfeld, Amin Sakzad, VietVo](javascript:void(0);" \o "Ron Steinfeld)

**ABSTRACT**: Symmetric Searchable Encryption (SSE) has received wide attention due to its practical application in searching on encrypted data. Beyond search, data addition and deletion are also supported in dynamic SSE schemes. Unfortunately, these update operations leak some information of updated data. To address this issue, forward-secure SSE is actively explored to protect the relations of newly updated data and previously searched keywords. On the contrary, little work has been done in backward security, which enforces that search should not reveal information of deleted data. In this paper, we propose the first practical and non-interactive backward-secure SSE scheme. In particular, we introduce a new form of symmetric encryption, named symmetric puncturable encryption (SPE), and construct a generic primitive from simple cryptographic tools. Based on this primitive, we then present a backward-secure SSE scheme that can revoke a server's searching ability on deleted data. We instantiate our scheme with a practical puncturable pseudorandom function and implement it on a large dataset. The experimental results demonstrate its efficiency and scalability. Compared to the state-of-the-art, our scheme achieves a speedup of almost 50x in search latency, and a saving of 62% in server storage consumption.

# 3.Title: Power Range: Forward Private Multi-Client Symmetric Searchable Encryption with Range Queries Support

# Author: [Alexandros Bakas](https://ieeexplore.ieee.org/author/37088528052); [Antonis Michalas](https://ieeexplore.ieee.org/author/37705403600)

**ABSTRACT:** Symmetric Searchable encryption (SSE) is an encryption technique that allows users to search directly over their outsourced encrypted data while preserving the privacy of both the files and the queries. In this paper, we present Power Range - a dynamic SSE scheme (DSSE) that supports range queries in the multi-client model. We prove that our construction captures the very crucial notion of forward privacy in the sense that additions and deletions of files do not reveal any information about the content of past queries. Finally, to deal with the problem of synchronization in the multi-client model, we exploit the functionality offered by Trusted Execution Environments and Intel’s SGX.

# 4.Title: SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems

# Author: [Mingwu Zhang](https://ieeexplore.ieee.org/author/37086036289); [Yu Chen](https://ieeexplore.ieee.org/author/37088526584); [Jiajun Huang](https://ieeexplore.ieee.org/author/37086446769)

# ABSTRACT: Cloud computing provides an appearing application for compelling vision in managing big-data files and responding queries over a distributed cloud platform. To overcome privacy revealing risks, sensitive documents and private data are usually stored in the clouds in a cipher-based manner. However, it is inefficient to search the data in traditional encryption systems. Searchable encryption is a useful cryptographic primitive to enable users to retrieve data in ciphertexts. However, the traditional searchable encryptions provide lower search efficiency and cannot carry out fuzzy multikeyword queries. To solve this issue, in this article, we propose a searchable encryption that supports privacy-preserving fuzzy multikeyword search (SE-PPFM) in cloud systems, which is built by asymmetric scalar-product-preserving encryptions and Hadamard product operations. In order to realize the functionality of efficient fuzzy searches, we employ Word2vec as the primitive of machine learning to obtain a fuzzy correlation score between encrypted data and queries predicates. We analyze and evaluate the performance in terms of token of multikeyword, retrieval and match time, file retrieval time and matching accuracy, etc. The experimental results show that our scheme can achieve a higher efficiency in fuzzy multikeyword ciphertext search and provide a higher accuracy in retrieving and matching procedure.

# 5.Title:  Efficient Dynamic Searchable Encryption with Forward Privacy

**Author**: [Mohammad Etemad](https://arxiv.org/search/cs?searchtype=author&query=Etemad%2C+M), [Alptekin Küpçü](https://arxiv.org/search/cs?searchtype=author&query=K%C3%BCp%C3%A7%C3%BC%2C+A), [Charalampos Papamanthou](https://arxiv.org/search/cs?searchtype=author&query=Papamanthou%2C+C), [David Evans](https://arxiv.org/search/cs?searchtype=author&query=Evans%2C+D)

**ABSTRACT:** Searchable symmetric encryption (SSE) enables a client to perform searches over its outsourced encrypted files while preserving privacy of the files and queries. Dynamic schemes, where files can be added or removed, leak more information than static schemes. For dynamic schemes, forward privacy requires that a newly added file cannot be linked to previous searches. We present a new dynamic SSE scheme that achieves forward privacy by replacing the keys revealed to the server on each search. Our scheme is efficient and parallelizable and outperforms the best previous schemes providing forward privacy, and achieves competitive performance with dynamic schemes without forward privacy. We provide a full security proof in the random oracle model. In our experiments on the Wikipedia archive of about four million pages, the server takes one second to perform a search with 100,000 results.