**LITERATURE SURVEY**

**1) Practical Attributebased Multi-Keyword Search Scheme In Mobile Crowdsourcing**

**AUTHORS:** Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li,

Cloud-based mobile crowd-sourcing has been an attractive solution to provide data storage and share services for resource-limited mobile devices in a privacy-preserving manner, but how to enable mobile users to issue search queries and achieve fine-grained access control over ciphertexts simultaneously is still a big challenge for various circumstances. Although the ciphertext-policy attribute-based keyword search technology combining attribute-based encryption with searchable encryption has become a hot research topic, it just deals with equivalent attributes rather than more practical attribute comparisons, like “greater than” or “less than.” In this paper, we devise a practical cryptographic primitive called attribute-based multi-keyword search scheme to support comparable attributes through utilizing 0-encoding and 1-encoding. Formal security analysis proves that our scheme is selectively secure against chosen-keyword attack in generic bilinear group model and extensive experiments using real-world dataset demonstrate that our scheme can drastically decrease both computational and storage costs.

**2) Practical techniques for searches on encrypted data**

**AUTHORS:** D. X. Song, D. Wagner, and A. Perrig

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

**3) Searchable symmetric encryption: improved definitions and efficient constructions**

**AUTHORS:** R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky,

Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties: Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per returned document is constant as opposed to linear in the size of the data. Both solutions enjoy stronger security guarantees than previous constant-round schemes. In fact, we point out subtle but serious problems with previous notions of security for SSE, and show how to design constructions which avoid these pitfalls. Further, our second solution also achieves what we call *adaptive* SSE security, where queries to the server can be chosen adaptively (by the adversary) during the execution of the search; this notion is both important in practice and has not been previously considered. Surprisingly, despite being more secure and more efficient, our SSE schemes are remarkably simple. We consider the simplicity of both solutions as an important step towards the deployment of SSE technologies.As an additional contribution, we also consider *multi-user* SSE. All prior work on SSE studied the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in the multi-user setting, and present an efficient construction that achieves better performance than simply using access control mechanisms.

**4) Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage.**

**Authors:** J. Li, Y. Shi, and Y. Zhang

To protect the sensitive data outsourced to cloud server, outsourcing data in an encrypted way has become popular nowadays. However, it is not easy to find the corresponding ciphertext efficiently, especially the large ciphertext stored on cloud server. Besides, some data owners do not want those users who attempt to decrypt to know the sensitive access structure of the ciphertext because of some business or private reasons. In addition, the user attributes revocation and key updating are important issues, which affect application of ciphertext‐policy attribute‐based encryption (CP‐ABE) in cloud storage systems. To overcome the previous problems in cloud storage, we present a searchable CP‐ABE with attribute revocation, where access structures are partially hidden so that receivers cannot extract sensitive information from the ciphertext. The security of our scheme can be reduced to the decisional bilinear Diffie–Hellman (DBDH) assumption and decisional linear (DL) assumption.

**5)Attribute based keyword search over hierarchical data in cloud computing.**

**AUTHORS:** Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang

Searchable encryption (SE) has been a promising technology which allows users to perform search queries over encrypted data. However, the most of existing SE schemes cannot deal with the shared records that have hierarchical structures. In this paper, we devise a basic cryptographic primitive called as attribute-based keyword search over hierarchical data (ABKS-HD) scheme by using the ciphertext-policy attribute-based encryption (CP-ABE) technique, but this basic scheme cannot satisfy all the desirable requirements of cloud systems. The facts that the single keyword search will yield many irrelevant search results and the revoked users can access the unauthorized data with the old or outdated secret keys make this basic scheme not scale well in practice. To this end, we also propose two improved schemes (ABKS-HD-I,ABKS-HD-II) for the sake of supporting multi-keyword search and user revocation, respectively. In contrast with the state-of-the-art attribute-based keyword search (ABKS) schemes, the computation overhead of our schemes almost linearly increases with the number of users' attributes rather than the number of attributes in systems. Formal security analysis proves that our schemes are secure against both chosen-plaintext attack (CPA) and chosen-keyword attack (CKA) in the random oracle model. Furthermore, empirical study using a real-world dataset shows that our schemes are feasible and efficient in practical applications.