Searching on Encrypted Data

Eu-Jin Goh
eujin@cs.stanford.edu

November 25, 2003

1 Summary

There are currently three solutions: Searchable Symmetric Key Encryption (SSKE) [3], Searchable Public Key Encryption (SPKE) [1], and Secure Indexing [2].

SSKE and SPKE are encryption schemes that induce structure onto ciphertext so that a user can, given a trapdoor for a word, search the ciphertext for that word. Note that the user cannot deduce the word from the trapdoor. SSKE or SPKE requires linearly scanning all the ciphertext on a search.

Secure Indexing provides a solution to the problem of securely indexing documents so that a user, given a trapdoor, can search on the documents using the index in $O(1)$ time per document. The index has the security property that an adversary learns nothing about a document from its index other than what it already knows from previous query results or other channels. Consider a document P containing n words, of which an adversary already knows m words and wants information about the $n - m$ unknown words. We call the set of $n - m$ unknown words W. Even when the adversary is given plain text access to all other documents except on W, and is also allowed to make arbitrary queries of its choice on any word except those in W, the adversary still cannot obtain any information about any word in W from P's index.

Open Problem. There is at least one outstanding problem — The current index solution is $O(1)$ per document. There are inelegant extensions to the basic index construction that search over the entire set of documents. Construct elegant indexes that allow $O(1)$ search over the entire database.

References

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Searchable public key encryption. Cryptology ePrint Archive, Report 2003/195, Sep 2003.
`http://eprint.iacr.org/2003/195/`.

[2] E.-J. Goh. Secure indexes for efficient searching on encrypted compressed data. Cryptology ePrint Archive, Report 2003/216, Sep 2003.
`http://crypto.stanford.edu/ eujin/papers/encryptsearch/`.

[3] D. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 44–55. IEEE, May 2000.