Searchable Encryption Supporting General Boolean Expression Queries

Tarik Moataz[1] and Abdullatif Shikfa[2]

[1] Telecom Bretagne, Rennes, France,
tarik.moataz@telecom-bretagne.eu
[2] Bell Labs Research, Alcatel-Lucent, Nozay France,
abdullatif.shikfa@alcatel-lucent.com

Abstract. We present in this poster a symmetric searchable encryption scheme supporting general boolean search.
Keywords. Searchable encryption, boolean expressions, keyword search.

Searchable encryption is a mechanism that allows a user to store encrypted documents in an outsourced server, and later on query for some of these documents that match a given keyword. All these operations are performed with encrypted data, meaning both the documents and the queries are encrypted in such a way as to minimize leaked information: the server is considered to be semi-honest or honest-but-curious. Searchable encryption is an active research area and has witnessed several interesting schemes since the beginning of the 2000's, and in particular R.Curtmola et al. presented a construction which is asymptotically optimal with respect to search complexity. However, most prior works focused only on single keyword query and thus single keyword searches.

We target a more general model, which encompasses all basic boolean searches -the disjunction, the conjunction and the negation- over encrypted data at the same time. We propose a first construction of symmetric searchable encryption that supports generic boolean search over encrypted data which consists of four algorithms: Gen, Enc, $Query$ and $Test$. The construction is based on an original idea of considering keywords as vectors and using the Gram-Schmidt process to orthogonalize and then orthonormalize them. It further makes use of a very efficient operation, the inner product, to perform searches at the server side. The inner product indeed leverages the orthonormalized keywords to efficiently test if a boolean expression query matches the label corresponding to an encrypted document or not. The label construction consists on the orthonormalized keywords sum, while the queries sent for retrieving encrypted documents are further randomized to guarantee the security of our scheme. As the keywords need to be orthonormalized their size n is necessarily bigger than their number (otherwise we need to pad them). Hence, if the size of orthonormalized keywords is equal to n, then the size of any arbitrary query will be equal to n, the same follows for the size of labels. The details of the scheme are presented in [1].

References

1. T. Moataz and A. Shikfa. Boolean symmetric searchable encryption. *to appear in AsiaCCS*, 2013.