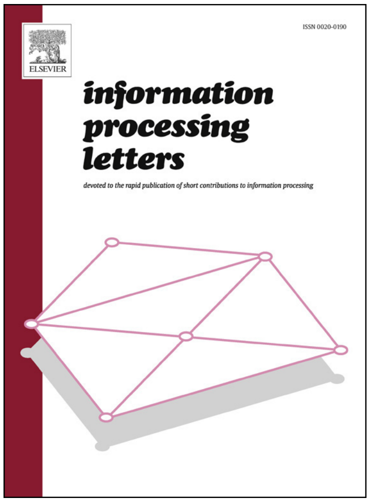
# On query result integrity over encrypted data

Ertem Esiner, Anwitaman Datta


ISSN 0020-0190
ELSEVIER
information processing letters
devoted to the rapid publication of short contributions to information processing

PII: S0020-0190(17)30032-7
DOI: http://dx.doi.org/10.1016/j.ipl.2017.02.005
Reference: IPL 5510

To appear in: *Information Processing Letters*

Received date: 15 June 2015
Revised date: 4 February 2017
Accepted date: 21 February 2017

# On query result integrity over encrypted data

Ertem Esiner, Anwitaman Datta

*Nanyang Technological University*

**Abstract**

We leverage on authenticated data structures to guarantee correctness and completeness of query results over encrypted data. Our contribution is in bridging two independent lines of work (searchable encryption, and provable data possession) resulting in a general purpose technique, which does so without increasing the client storage overhead, while only a small token and a data structure is added to the server side (in comparison to a base searchable encryption without mechanisms for determining result integrity), where the data structure can simultaneously also be used for integrity checks on the stored data.

*Keywords:* searchable encryption, result completeness & correctness, integrity, byzantine servers.

## 1. Introduction

With the proliferation of data outsourcing in recent years, there has been immense associated security concerns. Intertwined with these security concerns are aspects of functionality. Broadly, the basic security concerns can be seen in the context of the CIA-triad (confidentiality, integrity and availability).

Confidentiality can arguably be achieved using encryption, but it interferes with functionality. This has triggered research on searchable encryption [1, 2, 3, 4], where the challenge is between the degree of confidentiality and flexibility. Consequently, research on fuzzy search [5, 6] to facilitate approximate queries has gained recent attention.

Another broad area of research revolves around the integrity of outsourced data [7, 8, 9]. The emphasis in these works is to verify whether the data that has been outsourced has been correctly retained at the third party.

This work is at the confluence of these two broad areas, and proposes a generic technique to determine the correctness and completeness of individual query results when (fuzzy) searchable encryption is deployed. Note that this is distinct from determining the integrity of the whole outsourced data. There are several new searchable encryption schemes, where verifiability of the query responses is considered [10, 11, 12, 13, 14], however these existing works are protocol specific and are not readily portable.

With respect to typical searchable encryption schemes, our approach introduces two additional storage overheads. First, the server needs to keep a hash value per keyword. Second, the server needs to keep a data structure constructed over the data blocks. The data structure however simultaneously amortizes integrity