OST Review - Summary Report

David Cash, University of Chicago  
March 22, 2023

My review is primarily based on the design and analysis document for a cryptographic construction called OST dated February 2023, in addition to multiple meetings with the authors of the document. This document describes in detail the security goals of the behind OST, then gives detailed pseudocode for the main novel cryptographic algorithms. Finally it performs a theoretical security analysis with theorems and proofs that follow the standard “provable security” approach[[1]](#footnote-0).

My review did not involve a review of the larger Queryable Encryption product, including its implementation details, though the general setting was sketched for me for context.

In this summary I will provide some context for this type analysis and then summarize my findings and opinions about the results in this document.

**Context: Structured Encryption.** *Structured Encryption (StE)* is a family of cryptographic techniques for querying encrypted data. Since the foundational work over 13 years ago, (pioneered by Seny Kamara, an author of OST) thousands of research papers have been written exploring various aspects of StE, several startups have developed StE products, and there are likely many uses of StE that I’m not aware of.

StE typically achieves practical efficiency by allowing for controlled “leakage”, which is jargon for data or metadata that may be inferred by an adversary. When a new StE construction is proposed, it is typically straightforward to see if it is performant and usable. The more difficult question is whether it is secure, and particularly what the “leakage profile” the StE construction achieves, and if this leakage profile is sufficiently limiting.

**The security analysis of OST.** The main technical analysis of OST involves specifying a “leakage profile” with mathematical precision, and rigorously proving[[2]](#footnote-1) that OST leaks nothing more than this profile against “snapshot adversaries”, meaning those that obtain an entire image of the server after each operation.

The leakage profile of OST is ultimately very simple: Intuitively an adversary can only tell which fields of documents change between intrusions. OST does not reveal the contents of documents or their fields under any circumstances.

**My findings.** The analysis of OST was sound and correct. I found no significant errors or oversights in the provable security analysis.

The more nuanced question regards not the mathematical correctness of the analysis, but its ultimate practical meaning. Evaluating this aspect is more difficult, and I base my opinion on knowledge of the literature and experience rather than verifying proofs.

This simple leakage profile of OST strongly suggests that, against snapshot adversaries, it will be highly secure in practice. An adversary who obtains snapshots of the OST data structures and ciphertexts will only learn about the general sizes of the data, and can (for example) notice if an encrypted document has been added or deleted.

I could not think of any attacks that could exploit OST in practice. Only in some extreme and contrived instances is there even anything to exploit: An adversary may see that you uploaded a new document, and know the byte-length of its fields, but nothing further is inferrable. So if, say, the byte-length of a field is critical information, some care must be taken: If the only possible values of a field are “male” and “female”, then these may not be protected. However, even this is easily mitigated via standard techniques like padding or simply representing “male” and “female” as “M” and “F”.

A final note regards the choice of “snapshot adversaries”. As discussed in the design document, this choice is motivated by real threats against these systems: Misconfigured servers, rogue administrators, lost disks, etc. I believe this model corresponds well to these threats.

**Author bio:** I am an Associate Professor at the Department of Computer Science at the University of Chicago. My research is in theoretical and applied cryptography. I have worked on cryptographic algorithms, practical security analysis and attacks, and theoretical foundations of security. For the past decade I have focused on systems that work with encrypted data, including encrypted text search and encrypted databases. Further information about me and my work is available at [my web page](https://people.cs.uchicago.edu/~davidcash/) and my [Google Scholar page](https://scholar.google.com/citations?user=K0rhcG0AAAAJ&hl=en).

1. C.f. Textbooks like <http://www.cs.umd.edu/~jkatz/imc.html> for context on this approach. [↑](#footnote-ref-0)
2. Such proofs actually come with clauses of the form “unless all encryption on the internet is catastrophically broken”. In the case of OST, these caveats are totally benign, even if quantum computers are developed. [↑](#footnote-ref-1)