1 Semantic Security against Adaptive Chosen Keyword Attack (IND1-CKA and IND2-CKA)

- **Proposed in:** [1].
- **Setup:** Each document has a search index.
- **Idea(IND1-CKA):** Given index of one of two documents containing equal number of keywords, the adversary should not be able to tell which document it comes from.
- **Modification(IND2-CKA):** The number of keywords in the two documents can be different.
- **Adversarial Power:** Obtain trapdoor of any keywords apart from those in the two documents, and query the keywords on other documents.
- **Shortcomings:** The trapdoor does not need to be secure, so anyone can generate it.

2 (Non-Adaptive Indistinguishability/Semantic Security for SSE (IND-CKA1)

- **Proposed in:** [2].
- **Idea:** Given two histories (database with a fixed number of queries), the challenger encrypts one of the trace (database and queries) into a view, and the adversary should not be able to tell which history it comes from. There is a restriction that the trace (document identifiers, document sizes, document containing a particular keyword, and search pattern) of the two histories are identical.
- **Order of quantifiers for semantic security:** For q (number of queries), for all adversaries, there exists a simulator, such that all functions on the histories are indistinguishable.

3 Adaptive Indistinguishability/Semantic Security for SSE (IND-CKA2)

- **Proposed in:** [2].
- **Idea:** Similar to above, except that the adversary is allowed to generate queries adaptively.

4 Variants of IND-CKA2

- **Bit adversary:** IND-CQA2 in [3].
- **Stronger IND-CQA2**: They require a simulator to work for all adversaries. The final adversary is a bit adversary. First appears in [4].
- **Random oracle (most recent and most popular):** Instead of fixing leakage in the definition, they are defined carefully and used as query oracles. Everything else follows IND-CQA2 closely. First appears in [5].

References

[1] Eu-Jin Goh. Secure indexes. Cryptology ePrint Archive, Report 2003/216, 2003. `http://eprint.iacr.org/2003/216`.

[2] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 06: 13th Conference on Computer and Communications Security*, pages 79–88, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press.

[3] Melissa Chase and Seny Kamara. Structured encryption and controlled disclosure. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 577–594, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany.

[4] Kaoru Kurosawa and Yasuhiro Ohtaki. UC-secure searchable symmetric encryption. In Angelos D. Keromytis, editor, *FC 2012: 16th International Conference on Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 285–298, Kralendijk, Bonaire, February 27 – March 2, 2012. Springer, Heidelberg, Germany.

[5] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. Cryptology ePrint Archive, Report 2012/530, 2012. `http://eprint.iacr.org/2012/530`.