Searchable Symmetric Encryption

Douglas Choi
CECS 579

Motivation

- ➔ growing demand for storage of confidential data
- ➔ use of third-party cloud storage solutions
- ➔ we primarily access data by search
- ➔ ***How do we search on encrypted data?***

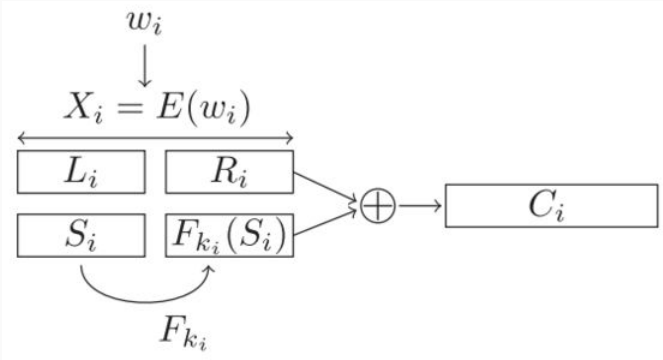
Adversary Model

- ➔ Access to *encryption oracle* and *search oracle*
- ➔ Security against adaptive chosen keyword attack - “CKA2”
  - ◆ Adversary cannot determine the contents of the documents or content of keyword…
    - even if adversary observes document ciphertext and search results
    - even if keywords are chosen by the adversary
    - even if keywords are chosen based on previous search history

Searchable Symmetric Encryption (SSE)

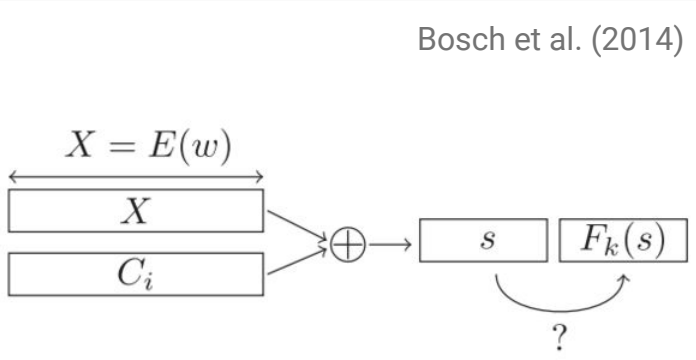
Song, Wagner, Perrig (SWP)

Encrypt



Search

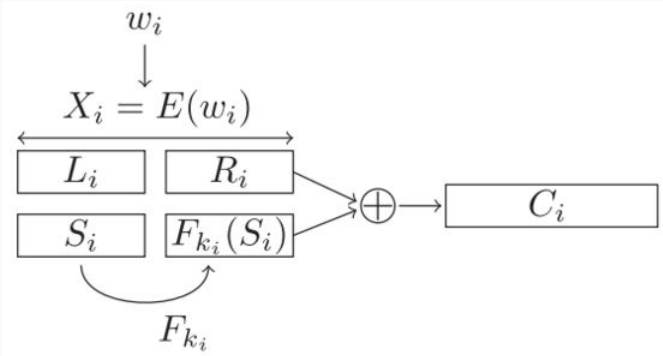
Bosch et al. (2014)



$X_i = E(w_i)$	deterministic encryption of w_i
S_i	pseudorandom value
k_i	key derived using a PRF of L_i
$F_{k_i}(S_i)$	hash of S_i using key k_i
C_i	ciphertext of w_i

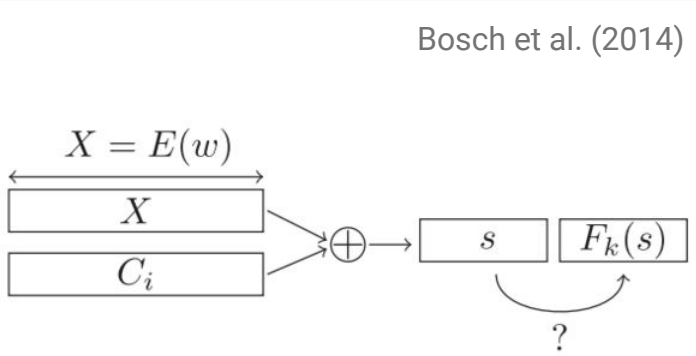
Song, Wagner, Perrig (SWP)

Encrypt



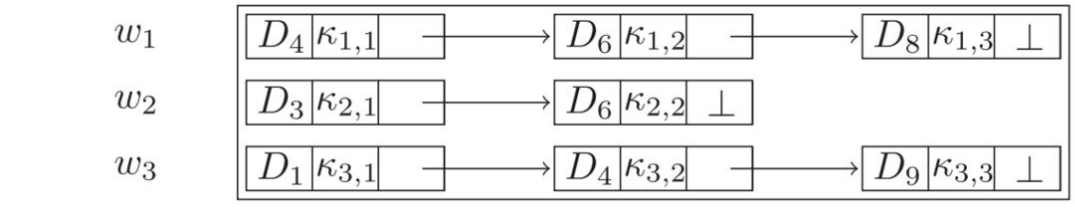
Search

Bosch et al. (2014)

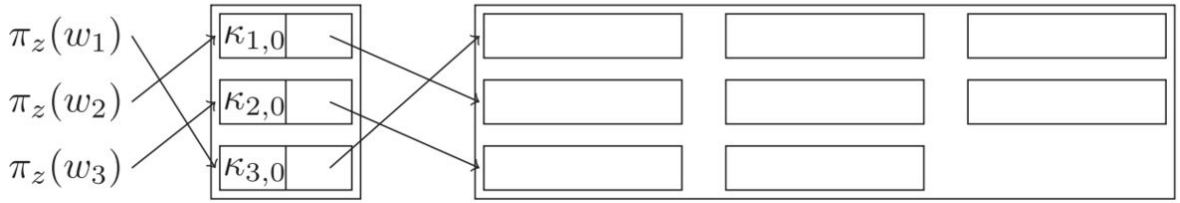


- ➔ Slow search time: *O(documents x words)*
- ➔ This is not CKA2 secure because can learn the words using frequency analysis.

Curtmola, Garay, Kamara (CGK)



(a) CGK$^+$: Linked lists L_i

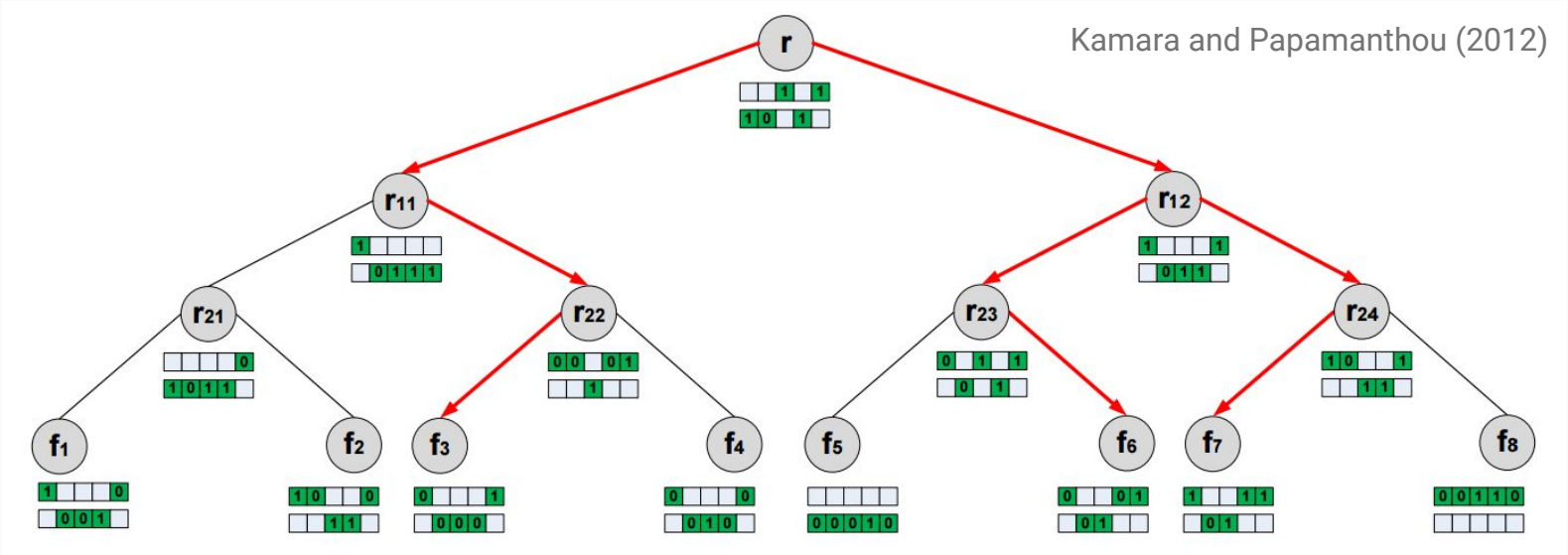


(b) CGK$^+$: Index table T and encrypted linked lists L_i

- ➔ Inverted index
- ➔ Consists of a linked list per distinct keyword
- ➔ Each node contains the document id and the key used to encrypt the next node
- ➔ Consists of a lookup table that maps the value of a pseudorandom permutation to the key and pointer to the first node

Bosch et al. (2014)

Parallel and Dynamic SSE - Kamara, Papamanthou (KP)



- ➔ Uses a data structure called keyword red-black (KRB) trees
- ➔ Dynamic: able to add, delete, and update existing files

Comparisons

scheme	dynamism	security	search time	index size
SWP	static	CPA	O(mn)	N/A
CGK	static	CKA	O(r)	O(m + n)
KP	dynamic	CKA	O(r log n)	O(nm)

n = number of documents
m = number of keywords
r = number of documents containing keyword w

Current Research

- ➔ Many different (and very complex) schemes under active research
- ➔ How to extend this to multiple writers and multiple readers
- ➔ How to improve search time and storage
- ➔ How to query for more complex search queries
- ➔ Deterministic trapdoors still reveal access patterns and search patterns

References

1. Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical Techniques for Searches on Encrypted Data. In 2000 Proceedings of the 2000 IEEE Symposium on Security and Privacy. 2000.

2. Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. In 13th ACM Conference on Computer and Communications Security Proceedings. 79 - 88. October, 2006.

3. Seny Kamara and Charalampos Papamanthou. Parallel and Dynamic Searchable Symmetric Encryption. Financial Cryptography and Data Security. 2013.

4. Christoph Bosch, Pieter Hartel, Willem Jonker, and Andres Peter. A Survey of Provably Secure Searchable Encryption. In ACM Computing Surveys, Vol. 47, No. 2, Article 18. August, 2014.