On the Encipherment of Search Trees and Random Access Files.

Rudolf Bayer, J. K. Metzger: On the Encipherment of Search Trees and Random Access Files. TODS 1(1): 37-52(1976)

```
@article{DBLP:journals/tods/BayerM76,
  author    = {Rudolf Bayer and
               J. K. Metzger},
  title     = {On the Encipherment of Search Trees and Random Access Files},
  journal   = {TODS},
  volume    = {1},
  number    = {1},
  year      = {1976},
  pages     = {37-52},
  ee        = {db/journals/tods/BayerM76.html},
  bibsource = {DBLP, http://dblp.uni-trier.de}
}
```

Abstract

The securing of information in indexed, random access files by means of privacy transformations must be considered as a problem distinct from that for sequential files. Not only must processing overhead due to encrypting be considered, but also threats to encipherment arising from updating and the file structure itself must be countered. A general encipherment scheme is proposed for files maintained in a paged structure in secondary storage. This is applied to the encipherment of indexes organized as B-trees; a B-tree is a particular type of multiway search tree. Threats to the encipherment of B-trees, especially relating to updating, are examined, and countermeasures are proposed for each. In addition, the effect of encipherment on file access and update, on paging mechanisms, and on files related to the enciphered index are discussed. Many of the concepts presented may be readily transferred to other forms of multiway index trees and to binary search trees.

Joint ACM SIGMOD / IEEE Computer Society Anthology

CDROM Version: Load the CDROM "**Volume 3 Issue 1, TODS 1976-1990**" and ...

- Windows: Click the letter of your CD drive
  A B C **D** **E** F G H I J K L M N O P Q R S T U V W X Y Z
- Mac: Click here
- UNIX/LINUX: mount the CD and click on the path of your *mount point*:
  /Anthology/An3-1 or /cdrom

DVD Version: Load **ACM SIGMOD Anthology DVD 2**" and ...

- Windows: Click the letter of your CD drive
  A B C **D** **E** F G H I J K L M N O P Q R S T U V W X Y Z
- Mac: Click here
- UNIX/LINUX: mount the DVD and click on the path of your *mount point*: /Anthology/aDVD2 or /dvd

Conference Abstract

Rudolf Bayer, J. K. Metzger: On the Encipherment of Search Trees and Random Access Files. VLDB 1975: 452

References

[1]
Rudolf Bayer, Edward M. McCreight: Organization and Maintenance of Large Ordered Indices. Acta Informatica 1: 173-189(1972)

[2]
...

[3]
Robert S. Fabry: Capability-Based Addressing. CACM 17(7): 403-412(1974)

[4]
...

[5]
Theodore D. Friedman, Lance J. Hoffman: Execution Time Requirements for Encipherment Programs. CACM 17(8): 445-449(1974)

[6]
Donald E. Knuth: The Art of Computer Programming, Volume III: Sorting and Searching. Addison-Wesley 1973, ISBN 0-201-03803-X

[7]
...

[8]
...

[9]
...

[10]
...

[11]
...

Referenced by

1. Thomas Hardjono, Jennifer Seberry: Search Key Substitution in the Encipherment of B-Trees. VLDB 1990: 50-58
2. Douglas Comer: The Ubiquitous B-Tree. ACM Computing Surveys 11(2): 121-137(1979)
3. David K. Hsiao, Douglas S. Kerr, Stuart E. Madnick: Privacy and Security of Data Communications and Data Bases. VLDB 1978: 55-67
4. Rudolf Bayer, Karl Unterauer: Prefix B-Trees. TODS 2(1): 11-26(1977)

ACM SIGMOD Anthology - DBLP: [Home | Search: Author, Title | Conferences | Journals]