ABSTRACT

The enabling key block (EKB) used in an encrypted key distributing constitution of a tree structure is generated by reconstructing a simplified 2-branch or multi-branch type tree with a terminal node or leaf which can decrypt as the lowest stage, and on the basis of only the key corresponding to a node or a leaf of the reconstructed hierarchical tree. Further, a tag as discrimination data at a tree position of an encrypted key stored in EKB is stored. The tag not only discriminates a position but stores data for judging presence of encrypted key data within EKB. A considerable reduction in data quantity is realized, and decrypting process in a device is also simplified. Thus, an information processing system and method capable of reducing data quantity of an enabling key block (EKB) used in an encrypted key constitution of a tree structure is realized.