

ABSTRACT

A block key to encrypt block data is generated using an ATS (arrival time stamp) appended to each of TS (transport stream) packets included in a transport stream correspondingly to the arrival time of the TS packet. The ATS is a random data depending upon an arrival time, and so a block-unique key can be generated, which enhances the protection against data cryptanalysis. A block key is generated from a combination of an ATS with a key unique to a device, recording medium or the like such as a master key, disc-unique key, title-unique key or the like. Since an ATS is used to generate a block key, any area for storage of an encryption key for each block may not be provided in a recording medium.