

ABSTRACT

SYSTEM AND METHOD ENABLING PARALLEL PROCESSING OF HASH FUNCTIONS USING AUTHENTICATION CHECKPOINT HASHES

Systems and methods enabling parallel processing of hash functions are provided. A data string including a plurality of pieces arranged in an order is hashed using a hash function to determine a plurality of authentication checkpoint hashes associated with the pieces. To authenticate the data string, the pieces are grouped into sets, and the authentication checkpoint hash associated with the piece following all other pieces of that set in the order is associated with that set. The system simultaneously performs a separate hash process on each set. That is, the system hashes the pieces of that set using the hash function to determine a result hash, and compares that result hash with the authentication checkpoint hash associated with that set. The initial input to the hash function for the hash process for each set includes one of the pieces and either a default seed or an authentication checkpoint hash.

FIG. 3

