Title (en)

PROCESSING METHOD FOR MESSAGE INTEGRITY WITH TOLERANCE FOR NON-SEQUENTIAL ARRIVAL OF MESSAGE DATA

Title (de)

VERARBEITUNGSVERFAHREN FÜR NACHRICHTENINTEGRITÄT MIT TOLERANZ IN BEZUG AUF NICHTSEQUENZIELLE ANKUNFT VON NACHRICHTENDATEN

Title (fr)

PROCÉDÉ DE TRAITEMENT POUR L'INTÉGRITÉ DE MESSAGE AVEC UNE TOLÉRANCE POUR LA RÉCEPTION NON SÉQUENTIELLE DE DONNÉES DE MESSAGE

Publication

EP 2087635 A2 20090812 (EN)

Application

EP 07864586 A 20071119

Priority

- US 2007085092 W 20071119
- US 86033006 P 20061121
- US 97612607 A 20071022
- US 98440007 A 20071116

Abstract (en)

[origin: WO2008064153A2] One example embodiment of the present invention discloses a method for processing an application packet for transmission includes receiving a plurality of segments of the application packet in a byte stream, the byte stream including a plurality of blocks, creating a plurality of superblocks within the byte stream by grouping a number of the plurality of blocks within the byte stream, and creating first pseudorandom bits for the plurality of superblocks. The method also includes determining a block number and a superblock number for a beginning of each of the plurality of segments, determining a block number and a superblock number for an ending of each of the plurality of segments in the byte stream. The method further includes generating a partial tag for each of the plurality of segments in the byte stream based on the first pseudorandom bits associated with the block numbers and superblock numbers between the determined beginning and ending of the each of the plurality of segments in the byte stream, combining the partial tags including a last partial tag associated with a last segment of the application packet to create an accumulated tag, generating an authentication tag based on the accumulated tag and second pseudorandom bits, storing the authentication tag, and transmitting the plurality of segments including the authentication tag.

IPC 8 full level

H04L 9/00 (2006.01)

CPC (source: EP KR)

H04L 9/0631 (2013.01 - EP); **H04L 9/0643** (2013.01 - EP); **H04L 9/0656** (2013.01 - EP); **H04L 9/14** (2013.01 - KR); **H04L 9/32** (2013.01 - KR); H04L 2209/80 (2013.01 - EP)

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 2008064153 A2 20080529; **WO 2008064153 A3 20080904**; CN 101542962 A 20090923; CN 101542962 B 20131106; EP 2087635 A2 20090812; EP 2087635 A4 20170705; JP 2010510756 A 20100402; KR 101088549 B1 20111205; KR 20090071656 A 20090701

DOCDB simple family (application)

US 2007085092 W 20071119; CN 200780043064 A 20071119; EP 07864586 A 20071119; JP 2009538471 A 20071119; KR 20097010385 A 20071119