Title (en)

METHOD FOR GENERATING A SECRET OR A KEY IN A NETWORK

Title (de)

VERFAHREN ZUR ERZEUGUNG EINES GEHEIMNISSES ODER SCHLÜSSELS IN EINEM NETZWERK

Title (fr)

PROCÉDÉ POUR GÉNÉRER UN ÉLÉMENT SECRET OU UNE CLÉ DANS UN RÉSEAU

Publication

EP 3298721 A1 20180328 (DE)

Application

EP 16716541 A 20160413

Priority

- DE 102015209496 A 20150522
- EP 2016058103 W 20160413

Abstract (en)

[origin: WO2016188667A1] Disclosed is method for generating a secret or key in a network. The network comprises at least a first and a second subscriber and a common transmission channel between at least the first and second subscribers. The first subscriber can output at least a first value and a second value and the second subscriber can output at least the first value and the second value on the transmission channel, the first subscriber generating a first sequence of subscriber values and the second subscriber generating a second sequence of subscriber values in order for the transmission to occur largely synchronously on the transmission channel; and the first subscriber and the second subscriber each generate a common secret or a common key, the first subscriber doing so on the basis of information about the first sequence of subscriber values and on the basis of a sequence of superposed values resulting from a superposition of the second sequence of subscriber values onto the first sequence of subscriber values on the transmission channel, and the second subscriber doing so on the basis of information about the second sequence of subscriber values and on the basis of the sequence of superposed values resulting from the superposition of the second sequence of subscriber values onto the first sequence of subscriber values on the transmission channel. At certain intervals or in accordance with a detected sequence of superposed values, at least the first subscriber outputs at least one filler value outside the first sequence of subscriber values or the second subscriber outputs at least one filler value outside the second sequence of subscriber values onto the transmission channel such that an edge change or change in values occurs on the transmission channel.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP KR US)

H04L 9/0838 (2013.01 - EP KR US); **H04L 9/0861** (2013.01 - US); **H04L 9/12** (2013.01 - US); H04L 2209/84 (2013.01 - EP KR US)

Citation (search report)

See references of WO 2016188667A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

DE 102015209496 A1 20161124; CN 107624229 A 20180123; CN 107624229 B 20210330; EP 3298721 A1 20180328; JP 2018516019 A 20180614; KR 20180009753 A 20180129; US 10841085 B2 20201117; US 2018123786 A1 20180503; WO 2016188667 A1 20161201

DOCDB simple family (application)

DE 102015209496 A 20150522; CN 201680029361 A 20160413; EP 16716541 A 20160413; EP 2016058103 W 20160413; JP 2017560802 A 20160413; KR 20177033600 A 20160413; US 201615575839 A 20160413