Title (en)

METHOD OF XOR HOMOMORPHIC ENCRYPTION AND SECURE CALCULATION OF A HAMMING DISTANCE

Title (de)

VERFAHREN FÜR HOMOMORPHE XOR-VERSCHLÜSSELUNG UND SICHERE BERECHNUNG EINER HAMMING-DISTANZ

Title (fr)

PROCEDE DE CHIFFREMENT HOMOMORPHE POUR LE OU EXCLUSIF ET CALCUL SECURISE D'UNE DISTANCE DE HAMMING

Publication

EP 2951944 A1 20151209 (FR)

Application

EP 14701769 A 20140130

Priority

- FR 1350904 A 20130201
- EP 2014051759 W 20140130

Abstract (en)

[origin: WO2014118257A1] The invention concerns a method for encrypting a binary data item characterised in that it comprises the steps consisting of: - generating a public key and a private key, the public key being a sparse matrix comprising m rows and n columns, m being greater than the number I of bits of the binary data item, I being an integer strictly greater than 1, and the private key being a set of I indexed sets of integers between 1 and m such that for each set, the sum of the elements of the rows of the sparse matrix indexed by the elements of a set is zero, and - generating a binary sequence b comprising m bits, such that b=Mx+e+y in which o x is a random binary vector, o e is a random binary noise vector, and o y is a linear encoding of data item c. The invention also concerns a method for calculating a Hamming distance on data encrypted by the method of encryption.

IPC 8 full level

H04L 9/00 (2006.01); **H04L 9/30** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

H04L 9/008 (2013.01 - EP US); **H04L 9/0869** (2013.01 - US); **H04L 9/304** (2013.01 - EP US); H04L 9/3231 (2013.01 - EP US)

Citation (search report)

See references of WO 2014118257A1

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)

WO 2014118257 A1 20140807; EP 2951944 A1 20151209; FR 3001848 A1 20140808; FR 3001848 B1 20150109; US 2015365229 A1 20151217

DOCDB simple family (application)

EP 2014051759 W 20140130; EP 14701769 A 20140130; FR 1350904 A 20130201; US 201414764955 A 20140130