Title (en)

RING-BASED SIGNATURE SCHEME

Title (de)

SIGNATURSCHEMA AUF RINGBASIS

Title (fr)

SCHEMA DE SIGNATURE A BASE D'ANNEAUX

Publication

EP 1397884 A4 20060215 (EN)

Application

EP 02731656 A 20020503

Priority

- US 0214099 W 20020503
- US 28884101 P 20010504

Abstract (en)

[origin: WO02091664A1] A method and system for generating and verifying a digital signature of a message is provided. The digital signature includes digital signature polynomials. Two relatively prime ideals p and q of a ring R(102) are selected. A private key and the second ideal q are used to generate a public key. One or more message polynomials are generated based on the message to be signed. The digital signature polynomials are generated (110) using at least one of the message polynomials, at least one of the private key polynomials, and at least one of the ideals p and q, wherein the digital signature polynomials in unreduced form are not multiples of the private key polynomials in the ring R. The signature is then verified (116) by confirming that a deviation between at least one of the messae polynomials and at least one of the digital signature polynomials is less than a predetermined deviation threshold.

IPC 8 full level

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

CPC (source: EP)

H04L 9/3066 (2013.01); **H04L 9/3093** (2013.01); **H04L 9/3247** (2013.01); H04L 2209/80 (2013.01)

Citation (search report)

- [A] WO 9808323 A1 19980226 - NTRU CRYPTOSYSTEMS INC [US]
- [A] HOFFSTEIN J ET AL: "Optimization for NTRU", 11 September 2000, PUBLIC-KEY CRYPTOGRAPHY AND COMPUTATIONAL NUMBER THEORY, XX, XX, XP002990916
- See references of WO 02091664A1

Citation (examination)

- HOFFSTEIN, PIPHER, SILVERMAN: "NSS: The NTRU Signature Scheme", November 2000 (2000-11-01), USA, pages 1 - 30, Retrieved from the Internet <URL:http://www.ntru.com/cryptolab/pdf/nss.pdf> [retrieved on 20070828]
- MIRONOV, ILYA: "A Note on Cryptanalysis of the Preliminary Version of the NTRU Signature Scheme", 23 January 2001 (2001-01-23), USA, pages 1 - 6, XP007902930, Retrieved from the Internet <URL:http://eprint.iacr.org/2001/005> [retrieved on 20070828]

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

WO 02091664 A1 20021114; CN 1268086 C 20060802; CN 1462520 A 20031217; EP 1397884 A1 20040317; EP 1397884 A4 20060215; JP 2004526387 A 20040826; JP 4053431 B2 20080227

DOCDB simple family (application)

US 0214099 W 20020503; CN 02801519 A 20020503; EP 02731656 A 20020503; JP 2002588007 A 20020503