Title (en)

SECURE USER IDENTIFICATION BASED ON RING HOMOMORPHISMS

Title (de)

AUF EINEM RINGHOMOMORPHISMUS BASIERENDE SICHERE BENUTZERIDENTIFIZIERUNG

Title (fr)

IDENTIFICATION SURE D'UTILISATEUR SUR LA BASE D'HOMOMORPHISMES EN ANNEAU

Publication

EP 1190523 A4 20040804 (EN)

Application

EP 00957240 A 20000503

Priority

- US 0012025 W 20000503
- US 13219999 P 19990503

Abstract (en)

[origin: WO0101625A1] A method and system is disclosed for performing user identification, digital signatures and other secure communication functions based on ring homomorphisms (220). In one embodiment, a secure user identification technique is disclosed in which one of the system users, referred to as a Prover, randomly selects an element g from the set Rg. The Prover (230) evaluates the homomorphism O(g) (220) to another user referred to as the Verifier. The Verifier randomly selects a challenge element c from the set Rc. The Verifier transmits c to the Prover (230). The Prover (230) generates a response element h using the private key f and the elements c and g. The element h may be generated in the form g*(f +c*g) using addition + and multiplication * in the ring R; or more generally by choosing a set of elements gi, receiving a set of challenge elements ci, creating modified challenge elements dj from the challenge elements ci, transmitting the modified challenge elements di to the Verifier, and generating the response element h as a polynomial function of the secret key f and the selected elements gi, ci, and dj. The Verifier checks that the element h is in the set Rh. The Verifier also evaluates the homomorphism O (220) at the element h and compares the result O(h) to a function of O(g), O(c), and the public key O(f) (240) of the power.

IPC 1-7

H04L 9/30; H04L 9/00; H04L 9/32

IPC 8 full level

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

CPC (source: EP)

H04L 9/008 (2013.01); **H04L 9/3093** (2013.01); **H04L 9/3218** (2013.01); **H04L 9/3255** (2013.01)

Citation (search report)

- [A] FR 2737370 A1 19970131 - BULL CP8 [FR]
- [A] US 5740250 A 19980414 - MOH TZUONG-TSIENG [US]
- [A] US 5220606 A 19930615 - GREENBERG HAROLD [US]
- [X] J HOFFSTEIN, J. PIPHER, JH. SILVERMAN: "NTRU A Ring based Public Key Cryptosystem", SPRINGER-VERLAG, vol. CS, no. 1423, June 1998 (1998-06-01), Portland OR, pages i,1 - 22, XP002280479, Retrieved from the Internet <URL:http:www.ntru.com/cryptolab/articles.html> [retrieved on 20040420]
- See references of WO 0101625A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 0101625 A1 20010104; **WO 0101625 A9 20020613**; AU 6889100 A 20010131; EP 1190523 A1 20020327; EP 1190523 A4 20040804; IL 146350 A0 20020725

DOCDB simple family (application)

US 0012025 W 20000503; AU 6889100 A 20000503; EP 00957240 A 20000503; IL 14635000 A 20000503