9802592-7
RNWP's copy!

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 — A1

(11) International Publication Number: WO 97/16903

(43) International Publication Date: 9 May 1997 (09.05.97)

(21) International Application Number: PCT/NL96/00413

(22) International Filing Date: 23 October 1996 (23.10.96)

(30) Priority Data:
1001568 3 November 1995 (03.11.95) NL

(71)(72) Applicant and Inventor: BRANDS, Stefanus, Alfonsus [NL/NL]; Ina Boudier-Bakkerlaan 143 III, NL-3582 XW Utrecht (NL).

(74) Agent: EVELEENS MAARSE, P.; Arnold & Siedsma, Sweelinckplein 1, NL-2517 GK Den Haag (NL).

(81) Designated States: AM, AU, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TT, UA, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CRYPTOGRAPHIC METHODS FOR DEMONSTRATING SATISFIABLE FORMULAS FROM PROPOSITIONAL LOGIC

(57) Abstract

Cryptographic methods are disclosed, which allow a prover party, who holds a number of secrets, to demonstrate satisfiable formulas of propositional logic, wherein the atomic propositions are linear relations between the secrets. The demonstration reveals no more information than is contained in the formula itself. Some implementations allow an unlimited number of such demonstrations to be made, without revealing any additional information about the secrets, whereas other implementations ensure that the secrets, or some of the secrets, will be revealed, if a demonstration is performed more than a predetermined number of times. The demonstrations may be zero-knowledge proofs, or signed proofs.

