(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014020 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/IB2003/003187

(22) International Filing Date: 7 July 2003 (07.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02405658.2 29 July 2002 (29.07.2002) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NJ 10504 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CAMENISCH, Jan** [CH/CH]; Bahnhofstrasse 13, CH-8803 Rueschlikon (CH). **KOPROWSKI, Maciej** [PL/DK]; Snogebaeksvej 51, ST, -9, DK-8210 Aarhus V (DK).

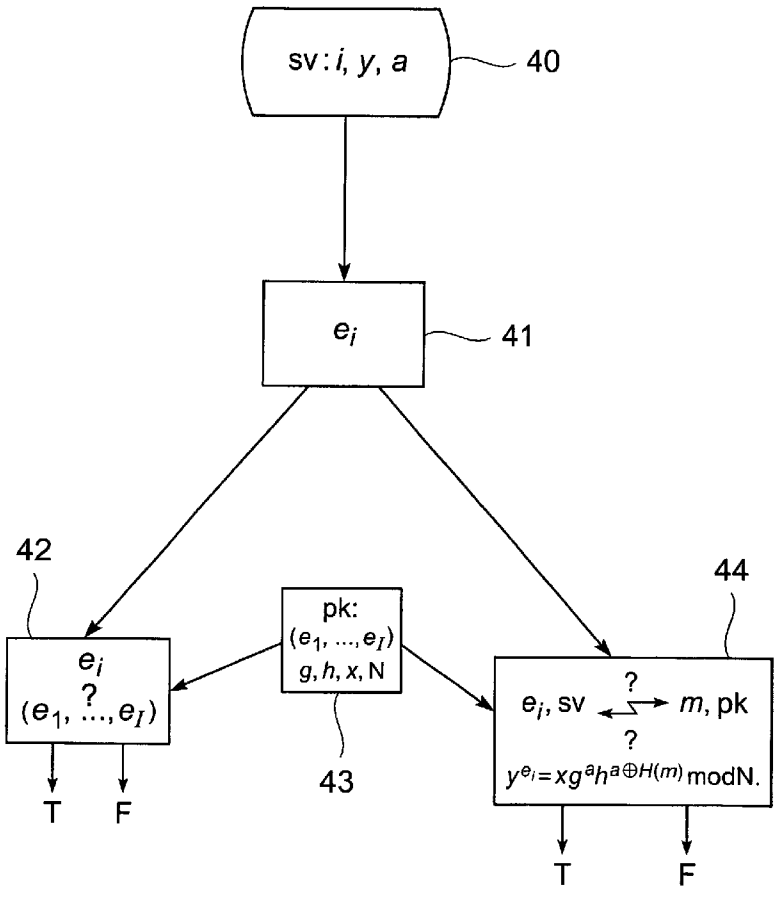
(74) Agent: **WILLIAMS, Julian, David**; International Business Machines Corporation, Saeumerstrasse 4/Postfach, CH-8803 Rueschlikon (CH).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: GROUPS SIGNATURE SCHEME



(57) Abstract: The presented methods form the basis of a forward-secure signature scheme that is provably secure. Moreover, the presented methods form also the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly. In general, each prepared signature carries an ascending index such that once an index is used, no lower index can be used to sign. Then, whenever an adversary breaks in, an honest signer can just announce the current index, e.g., by signing some special message with respect to the current index, as part of the revocation message for the current time period. It is then understood that all signatures made in prior time periods as well as all signatures make in the revoked period up to the announced index are valid, i.e., non-reputable.

WO 2004/014020 A1

ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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 receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.