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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2004 (15.04.2004)

PCT

(10) International Publication Number
WO 2004/032416 A1

(51) International Patent Classification[7]: H04L 9/32, 29/06

(21) International Application Number:
PCT/SG2002/000198

(22) International Filing Date: 30 August 2002 (30.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: LABORATORIES FOR INFORMATION TECHNOLOGY [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ZHOU, Jianying [CN/SG]; Blk 516 Jurong West Street 52#11-55, Singapore 640516 (SG). BAO, Feng [CN/SG]; 37 West Coast Park #04-06, Singapore 127653 (SG). DENG, Huijie, Robert [SG/SG]; 2 Namly Rise, Singapore 267110 (SG).

(74) Agent: GREENE-KELLY, James, Patrick; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

(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, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

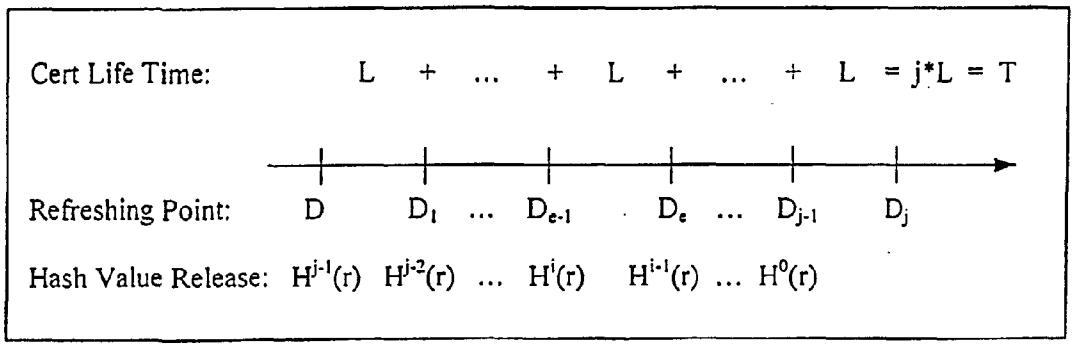
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

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.

(54) Title: PUBLIC KEY CRYPTOGRAPHY AND A FRAMEWORK THEREFOR



(57) Abstract: A method of performing a public/private key operation is disclosed comprising: generating a private and public key pair, the public key having a lifetime; selecting a plurality of intervals within the lifetime and a plurality of respective identifiers, each interval being associated with a said identifier; and having a trusted third party generate a public key certificate which includes the public key and a final identifier, the identifiers being selected so that it is relatively difficult to derive an identifier associated with a said interval from the final identifier but relatively easy to derive the final identifier from an identifier associated with a said interval, a said identifier being provided by a user with any matter signed or otherwise operated upon using the private key in the associated interval to confirm the validity of the certificate in that interval. A forward-secure digital signature scheme in which transactions for validity periods both before and after the current period remain secure even if the private key for the current period is compromised is also disclosed.

WO 2004/032416 A1