15/09/03
20030542 93

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082717 A1

(51) International Patent Classification[7]: H04L 9/28, G06F 7/00

(21) International Application Number: PCT/SG01/00077

(22) International Filing Date: 5 April 2001 (05.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **KENT RIDGE DIGITAL LABS** [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **YE, Dingfeng** [CN/SG]; State Key Lab of Information Security, P.O. Box 3908, Beijing 100039 (CN). **BAO, Feng** [CN/SG]; Parkview Condo #04-06, 37 West Coast Park, Singapore 127653 (CN). **DENG, Robert** [SG/SG]; 2 Namly Rise, Singapore 267110 (SG). **WU, Hongjun** [CN/SG]; Block 203 #05-09, Boon Lay Drive, Singapore 640203 (CN).

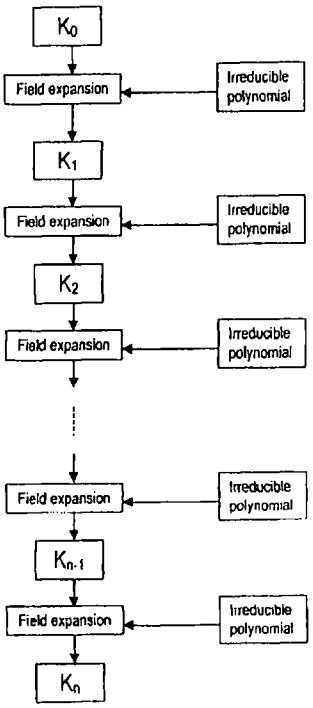
(74) Agent: **HELEN YEO & PARTNERS**; #33-00 UOB Plaza 1, 80 Raffles Place, Singapore 048624 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

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

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CONSTRUCTING EFFICIENT ELLIPTIC CURVE CRYPTOSYSTEMS



K_0: basic field with small number of elements

K_1: expansion field of K_0 by an irreducible polynomial of K_0

K_2: expansion field of K_1 by an irreducible polynomial of K_1

.....

K_n: expansion field of K_{n-1} by an irreducible polynomial of K_{n-1}

(57) Abstract: Methods and apparatus to construct finite fields over which efficient elliptic curve cryptosystems can be set up. Given a security parameter k, the said methods and apparatus consist of devices for carrying out operations in a small k_0-bit field k_0 and methods to successively build extension fields K_1 ; K_2, ..., K_t, where the extension K_1/K_0 has degree 2 or 3 and the other extensions K_i/K_{i-1} are quadratic, K_t is the final field over which elliptic curves are defined, and K_t has size $k_0 2^t$ or $3k_0 2^{t-1}$ just exceeding the said security parameter k.



162162



ACTION

WO 02/082717 A1

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.