

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

(19) World Intellectual Property Organization
International Bureau



G00002

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11360 A3

(51) International Patent Classification⁷: **H04L 9/30.**
G06F 7/72

(21) International Application Number: PCT/US01/23676

(22) International Filing Date: 26 July 2001 (26.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/627,927 28 July 2000 (28.07.2000) US

(71) Applicant: **ATMEL CORPORATION** [US/US]; 2325
Orchard Parkway, San Jose, CA 95131 (US).

(72) Inventor: **SABIN, Michael, John**; 883 Mango Avenue,
Sunnyvale, CA 94087 (US).

(74) Agents: **D'ALLESANDRO, Kenneth** et al.; Sierra Patent
Group, P.O. Box 6149, Stateline, NV 89449 (US).

(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, 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, 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, GQ, GW, ML, MR, NE, SN, TD,
TG).

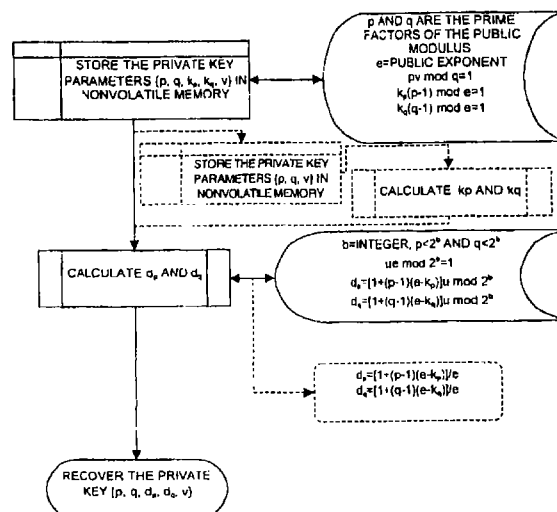
Published:

- 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

(88) Date of publication of the international search report:
13 June 2002

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: CRYPTOGRAPHY PRIVATE KEY STORAGE AND RECOVERY METHOD AND APPARATUS



162162

(57) Abstract: Disclosed herein is a system and method for storage and recovery of a private key in a cryptographic system by providing a parameterization of the private key that uses less storage space than the full CRT parameter set {p, q, d_p, d_q, v} and that provides better computational efficiency than the minimal parameter set {p, q}. Also disclosed is a system and method for storage and recovery of a private key in a cryptographic system by providing a parameterization of the private key that uses less storage space than the full non-CRT parameter set {n, d} and that provides better computational efficiency than the minimal parameter set {p, q}. Furthermore, disclosed herein is a means for computing the parameters d_p, d_q, and d in a manner such that the computational sequence is independent of the values of the prime factors p and q, thereby reducing vulnerability to attacks that exploit such dependence.