

(19) World Intellectual Property Organization
International Bureau



(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).

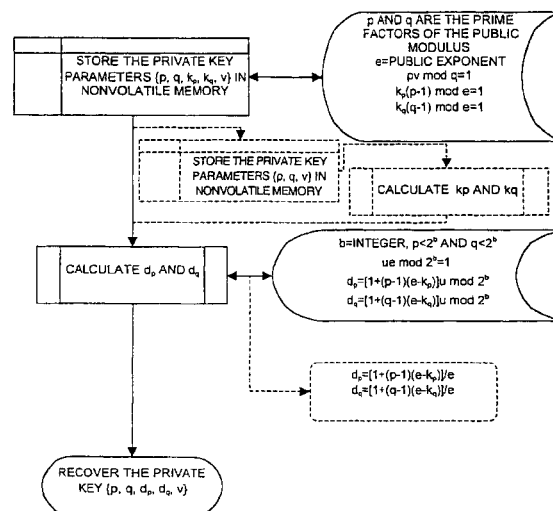
Published:

- 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 "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: CRYPTOGRAPHY PRIVATE KEY STORAGE AND RECOVERY METHOD AND APPARATUS



(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.

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 01/23676

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHAE HOON LIM, PIL JOONG LEE: "Sparse RSA Secret Keys and Their Generation" PROC. OF 3RD ANNUAL WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC'96), 'Online! August 1996 (1996-08), pages 117-131, XP002191771 Queen's University, Kingston, Ontario, Canada Retrieved from the Internet: <URL:citeseer.nj.nec.com> 'retrieved on 2002-02-28! page 120 -page 121 page 124 -page 125 page 127 -----	1-68

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

19 March 2002

Date of mailing of the international search report

04/04/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F