

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
4 March 2004 (04.03.2004)

PCT

(10) International Publication Number
WO 2004/019548 A1

(51) International Patent Classification⁷: **H04L 9/00**,
G06F 7/72

(21) International Application Number:
PCT/CA2003/001279

(22) International Filing Date: 25 August 2003 (25.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/228,151 26 August 2002 (26.08.2002) US

(71) Applicant (for all designated States except US): **MOSAID
TECHNOLOGIES INCORPORATED** [CA/CA]; 11
Hines Road, Kanata, Ontario K2K 2X1 (CA).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **ZAABAB, Hafid**
[CA/CA]; 5-2797 Baseline Road, Ottawa, Ontario K2H
7B5 (CA).

(74) Agent: **OGILVY RENAULT**; Suite 1600, 1981 McGill
College Avenue, Montreal, Québec H3A 2Y3 (CA).

(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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, SY, 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, 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 "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.*

(54) Title: METHOD AND APPARATUS FOR PROCESSING ARBITRARY KEY BIT LENGTH ENCRYPTION OPERATIONS
WITH SIMILAR EFFICIENCIES

(57) Abstract: A calculating apparatus, or system, having a plurality of stages, such as in a pipeline arrangement, has the clocking
rail or conductor positioned alongside the stages. With a large number, i.e., hundreds, of stages arranged in parallel sub-arrays, the
clocking conductor is snaked alongside the sub-arrays. In individual stages it is arranged that the shortest of the two calculations
taking place in a stage, takes place in the return path. An array can be divided into separate sections for independent processing.

WO 2004/019548 A1