PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30 | A1

(11) International Publication Number: WO 98/26536

(43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/22026

(22) International Filing Date: 8 December 1997 (08.12.97)

(30) Priority Data:
60/033,271 9 December 1996 (09.12.96) US
08/784,453 16 January 1997 (16.01.97) US

(71) Applicant: TANDEM COMPUTERS INCORPORATED [US/US]; 10435 North Tantau Avenue, Cupertino, CA 95014 (US).

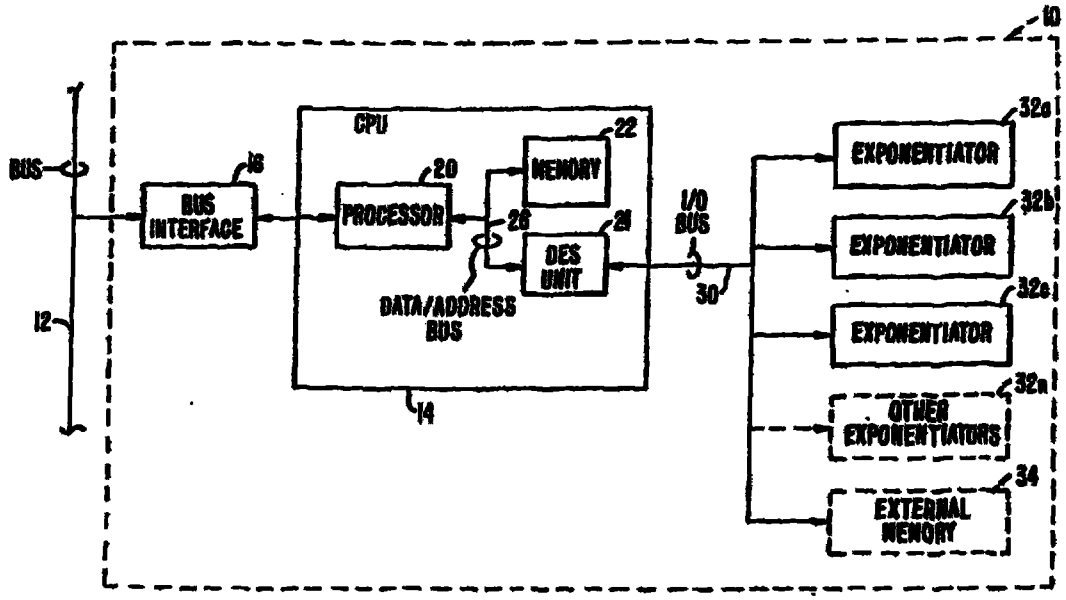
(72) Inventors: COLLINS, Thomas; 14890 Baranza Lane, Saratoga, CA 95075 (US). HOPKINS, Dale; 2425 Ric Drive, Gilroy, CA 95020 (US). LANGFORD, Susan; 1275 Poplar Avenue #101, Sunnyvale, CA 94086 (US). SABIN, Michael; 883 Mango Avenue, Sunnyvale, CA 94087 (US).

(74) Agents: BENNETT, Robert, J. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

(81) Designated States: AU, BR, CA, CN, GH, HU, ID, IL, JP, KP, KR, LT, LU, MX, NO, NZ, PL, PT, RU, SG, TR, UA, VN, YU, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD



(57) Abstract

The method and the apparatus improve public key encryption schemes that employ a composite number formed from three or more distinct primes. The apparatus includes a CPU (14), a processor (20), a memory (22), and a DES unit (24). The apparatus further includes an I/O bus (30), a plurality of exponentiators (33a, 33b, 33c, 33n), and an externel memory (34). In addition, the apparatus has a bus interface (16) for interfacing the apparatus with another bus (12).