86 9701083-9.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08, G07C 9/00	A1	**(11) International Publication Number:** WO 96/08093
		(43) International Publication Date: 14 March 1996 (14.03.96)

(21) International Application Number: PCT/CA95/00509

(22) International Filing Date: 6 September 1995 (06.09.95)

(30) Priority Data:

08/301,677	7 September 1994 (07.09.94)	US
08/512,491	8 August 1995 (08.08.95)	US

(71) Applicant: MYTEC TECHNOLOGIES INC. [CA/CA]; Suite 430, 10 Gateway Boulevard, Don Mills, Ontario M3C 3A1 (CA).

(72) Inventors: TOMKO, George, J.; Mytec Technologies Inc., Suite 430, 10 Gateway Boulevard, Don Mills, Ontario M3C 3A1 (CA). SOUTAR, Colin; Mytec Technologies Inc., Suite 430, 10 Gateway Boulevard, Don Mills, Ontario M3C 3A1 (CA). SCHMIDT, Gregory, J.; Mytec Technologies Inc., Suite 430, 10 Gateway Boulevard, Don Mills, Ontario M3C 3A1 (CA).

(74) Agent: FAGGETTER, Ronald, D.; Fetherstonhaugh & Co., Suite 2300, 439 University Avenue, Toronto, Ontario M5G 1Y8 (CA).

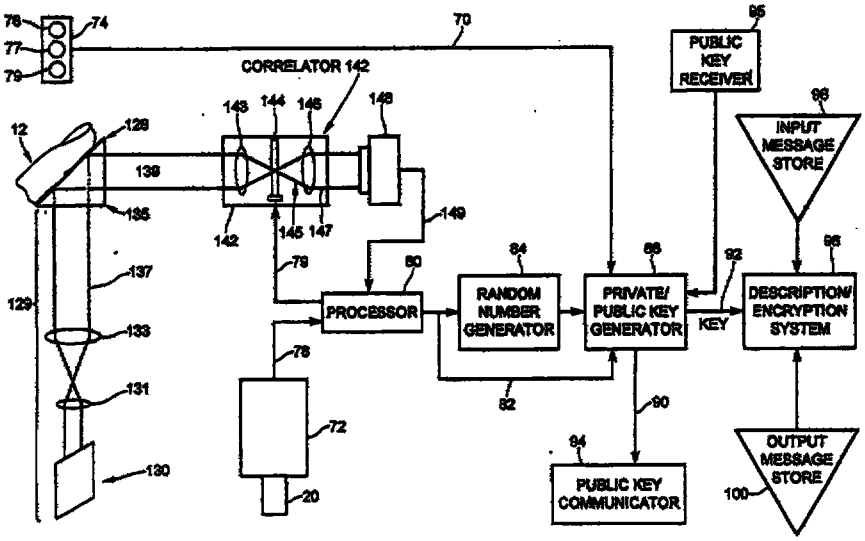
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

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: BIOMETRIC CONTROLLED KEY GENERATION



(57) Abstract

A key generation system is implemented as follows. In an enrolment apparatus, a unique number for use with PIN operated machines or public key cryptography system is generated by manipulation of fingerprint information of a subscriber. A filter is then generated which is a function both of the Fourier transform of the subscriber's fingerprint(s) and of the unique number. This filter is stored on a subscriber card. When the subscriber wishes to generate his key, he inputs his card to a card reader of an apparatus and places his finger(s) on a fingerprint input. The apparatus generates an optical Fourier transform from the fingerprint input. The Fourier transform signal is incident on to a spatial light modulator programmed with the filter information from the card. An inverse transform is generated from the filtered signal and this is used to regenerate the key that will be used as the PIN in a PIN operated device, or as the private key in a public key cryptography system.