9905612-9
IPAS

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L — A2

(11) International Publication Number: **WO 98/54864**

(43) International Publication Date: 3 December 1998 (03.12.98)

(21) International Application Number: PCT/US98/10392

(22) International Filing Date: 21 May 1998 (21.05.98)

(30) Priority Data:

08/864,839	28 May 1997 (28.05.97)	US
08/878,189	18 June 1997 (18.06.97)	US
08/920,504	29 August 1997 (29.08.97)	US
08/932,639	17 September 1997 (17.09.97)	US
08/959,351	28 October 1997 (28.10.97)	US

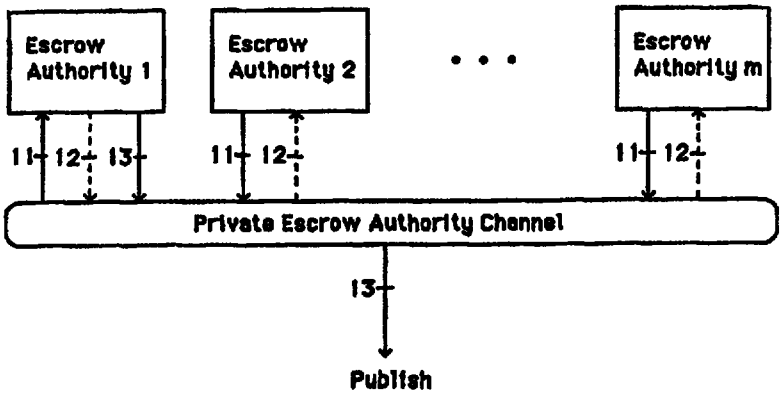
(71)(72) Applicants and Inventors: YOUNG, Adam, Lucas [US/US]; Apartment 12J, 535 West 110th Street, New York, NY 10025 (US). YUNG, Marcel, Mordechay [IL/US]; Apartment 4H, 605 West 112th Street, New York, NY 10025 (US).

(74) Agent: SCHWEITZER, Fritz, L., Jr.; Schweitzer Comman Gross, & Bondell LLP, 230 Park Avenue, New York, NY 10169 (US).

(81) Designated States: AL, AM, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, GW, HU, ID, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, UZ, VN, YU, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: AUTO-RECOVERABLE AUTO-CERTIFIABLE CRYPTOSYSTEMS



(57) Abstract

A method is provided for an escrow cryptosystem that is overhead–free, does not require a cryptographic tamper–proof hardware implementation (i.e., can be done in software), is publicly verifiable, and cannot be used subliminally to enable a shadow public key system. A shadow public key system is an unescrowed public key system that is publicly displayed in a covert fashion. The keys generated by the method are auto–recoverable and auto–certifiable (abbrev. ARC). The ARC Cryptosystem is based on a key generation mechanism that outputs a public/private key pair, and a certificate of proof that the key was generated according to the algorithm. Each generated public/private key pair can be verified efficient ly to be escrowed properly by anyone. The verification procedure does not use the private key. Hence, the general public has an efficient way of making sure that any given individual's private key is escrowed properly, and the trusted authorities will be able to access the private key if needed. Since the verification can be performed by anyone, there is no need for a special trusted entity, known in the art as a "trusted third party". The cryptosystem is overhead free since there is no additional protocol interact ion between the user who generates his or her own key, and the certification authority or the escrow authorities, in comparison to what is required to submit the public key itself in regular certified public key systems. Furthermore, the system is designed so that its internals can be made publicly scrutinizable (e.g., it can be distributed in source code form). This differs from any schemes which require that the escrowing device be tamper–proof hardware.