(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 October 2001 (04.10.2001)

PCT

(10) International Publication Number
WO 01/073694 A3

(51) International Patent Classification[7]: H04L 9/30

(21) International Application Number: PCT/US01/09550

(22) International Filing Date: 24 March 2001 (24.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/191,785	24 March 2000 (24.03.2000)	US
60/252,376	21 November 2000 (21.11.2000)	US
60/268,551	14 February 2001 (14.02.2001)	US

(71) Applicant *(for all designated States except US)*: **VOTE-HERE, INC.** [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NEFF, C., Andrew** [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).

(74) Agents: **DALEY-WATSON, Christopher, J.** et al.; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (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, US, 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, GW, ML, MR, NE, SN, TD, TG).

Published:

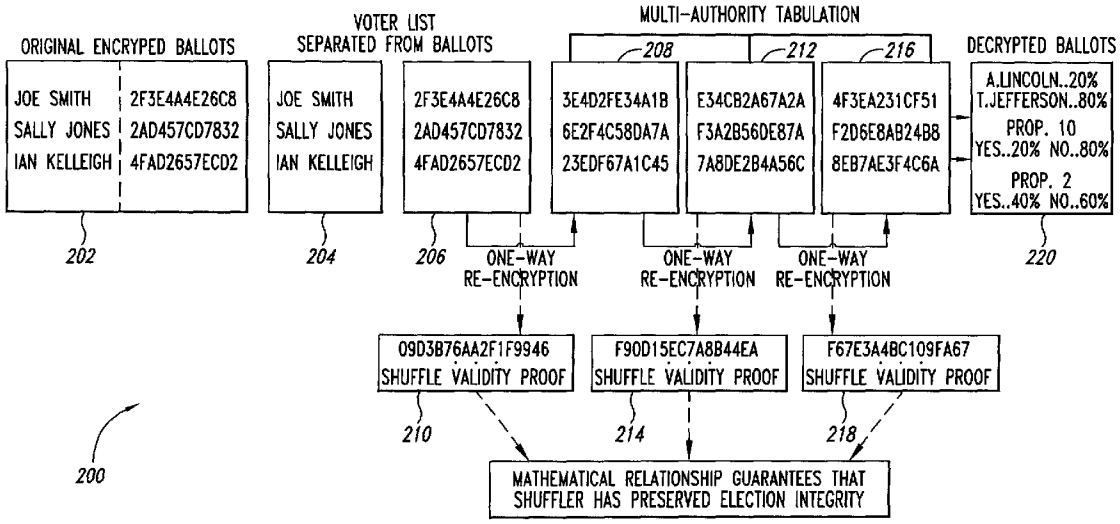
— *with international search report*

— *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:
6 February 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VERIFIABLE, SECRET SHUFFLES OF ENCRYPTED DATA, SUCH AS ELGAMAL ENCRYPTED DATA FOR SECURE MULTI-AUTHORITY ELECTIONS



(57) Abstract: A cryptographic process permits one to *verifiably* shuffle a series of input data elements. One or more authorities or individuals "shuffle", or "anonymize" the input data (e.g. public keys in discrete log form or ElGamal encrypted ballot data). The process includes a validity construction that prevents any one or more of the authorities or individuals from making any changes to the original data without being discovered by anyone auditing a resulting proof transcipt. The shuffling may be performed at various times. In the election example, the shuffling may be performed, e.g., after ballots are collected or during the registration, or ballot request phase of the election, thereby anonymizing the identities of the voters.

WO 01/073694 A3